

South Salt Lake Police Department

South Salt Lake PD Policy Manual

CHIEF OF POLICE DANIELLE CROYLE

Welcome to the South Salt Lake Police Departments policy manual. Employees of the South Salt Lake City Police Department are among the most visible representatives of City Government. To the majority of people, police officers are symbols of stability and authority upon whom they rely. The conduct of employees of the South Salt Lake City Police Department is closely scrutinized, and when actions are found to be excessive, unwarranted, or unjustified, they are criticized far more severely than the comparable conduct of persons in other walks of life. Since the employee's conduct, both on and off duty may reflect directly upon the Department, employees should conduct themselves in a manner, which does not bring discredit upon themselves, the Department or the City. These professional standards are designed to promote efficiency, positive discipline, enhance public relations and community support by setting for policies governing the conduct of all employees of the South Salt Lake City Police Department.

The procedures, regulations, sections, sentences, clauses and phrases of this manual are not intended to be in conflict with any laws, ordinance, or policy of the United State, the State of Utah, or the City of South Salt Lake, or its Departments. If any procedure, regulation, section, sentence, clause, or phase of of this policy manual to be invalid, such decision does not affect the validity of the remaining portions of the policy.

All employees of this Department shall familiarize themselves with the City of South Salt Lake Policies, Standards and Conduct, Department Written Directives, Orders of Policy, Ordinances of the City of South Salt Lake, Laws of the State of Utah or the United States. They shall conform to and obey the spirit and intent of these rulesany violation of these or other regulations whether on or off duty may subject and employee to disciplinary actions.

Violations of the City of South Salt Lake Policies, Standards and Conduct, Department Written Directives, Orders of Policy, Ordinances of the City of Salt Lake, Laws of the State of Utah, or the United States may subject offenders to disciplinary action up to and including termination. Action taken on violations depends on the degree of severity, record of the offender, and seriousness of the consequences of the action. It is the duty of every employee to take appropriate corrective action and/or report to the appropriate Division Commander via the proper chain of command, when she/he learns of a violation of the law, policy, procedure, orders, or other written directives.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

LAW ENFORCEMENT CODE OF ETHICS

As a Law Enforcement Officer, my fundamental duty is to serve mankind; to safeguard lives and property; to protect the innocent against deception, the weak against oppression or intimidation, and the peaceful against violence or disorder; and to respect the Constitutional rights of all men to liberty, equality and justice.

I will keep my private life unsullied as an example to all; maintain courageous calm in the face of danger, scorn, or ridicule; develop self-restraint; and be constantly mindful of the welfare of others. Honest in thought and deed in both my personal and official life, I will be exemplary in obeying the laws of the land and the regulations of my department. Whatever I see or hear of a confidential nature or that is confided to me in my official capacity will be kept ever secret unless revelation is necessary in the performance of my duty.

I will never act officiously or permit personal feelings, prejudices, animosities, or friendships to influence my decisions. With no compromise for crime and with relentless prosecution of criminals, I will enforce the law courteously and appropriately without fear or favor, malice or violence and never accepting gratuities.

I recognize the badge of my office as a symbol of public faith, and I accept it as a public trust to be held so long as I am true to the ethics of the police service. I will constantly strive to achieve these objectives and ideals, dedicating myself before God to my chosen profession...law enforcement.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

SOUTH SALT LAKE POLICE DEPARTMENT MISSION STATEMENT

The South Salt Lake Police Department is committed to enhancing the quality of life in our community by providing professional police services through TRUST, dignity and fidelity.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Table of Contents

Chief of Police Danielle Croyle.	1
Law Enforcement Code of Ethics.	2
South Salt Lake Police Department Mission Statement.	3
Chapter 1 - Law Enforcement Role and Authority.	9
100 - Law Enforcement Authority.	10
101 - Chief Executive Officer.	13
102 - Policy Manual.	14
103 - Professional Standards and Conduct.	17
104 - Oath of Office.	20
105 - Constitutional Safeguards - Investigations.	22
106 - Federal Law Enforcement or National Guard Assistance.	25
Chapter 2 - Organization and Administration.	26
200 - Staffing Levels.	27
201 - Organizational Structure and Responsibility.	28
202 - Electronic Mail.	34
203 - Administrative Communications.	36
204 - General Order.	39
205 - Retiree Concealed Firearms.	40
Chapter 3 - General Operations.	43
300 - Standards of Conduct.	44
301 - Bias-Based Policing.	53
302 - Officer Response to Calls.	56
303 - Use of Force.	60
304 - Use of Force Review Boards.	70
305 - Search and Seizure.	71
306 - Strip Search and/or Body Cavity Search.	77
307 - Control Devices and Techniques.	78
308 - Conducted Energy Device.	85
309 - Handcuffing and Restraints.	93
310 - Firearms.	97
311 - Domestic Violence.	106
313 - Officer-Involved Shootings and Deaths.	114
314 - Victim and Witness Assistance.	123
315 - Hate Crimes.	128
316 - Public Alerts.	130
317 - Adult Abuse.	135
318 - Missing Persons.	143
319 - Discriminatory Harassment.	156
320 - Child Abuse.	161

South Salt Lake Police Department

South Salt Lake PD Policy Manual

321 - Report Preparation.	167
322 - Media Relations.	171
323 - Subpoenas and Court Appearances.	176
324 - Reserve and Auxiliary Officers.	179
325 - Outside Agency Assistance.	188
326 - Registered Offender Information.	190
327 - Major Incident Notification.	193
328 - Death Investigation.	195
330 - Limited English Proficiency Services.	198
332 - Mandatory Employer Notification.	206
334 - Public Safety Video Surveillance System.	207
335 - Unmanned Aerial System.	211
336 - Communications to and from Field Officers.	215
337 - Youth Resource Officer Program.	219
338 - Child and Dependent Adult Safety.	221
339 - Volunteer Program.	225
340 - Off-Duty Law Enforcement Actions.	230
341 - Community Relations.	232
342 - Generative Artificial Intelligence Use.	237
343 - ADA Compliance.	242
344 - Vehicle Pursuits.	251
345 - Service Animals.	262
 Chapter 4 - Patrol Operations.	 265
400 - Patrol Function.	266
401 - Briefing.	269
402 - Canines.	271
403 - Crime and Disaster Scene Integrity.	283
404 - Special Weapons and Tactics Unit (SWAT).	285
405 - Ride-Along Program.	290
406 - Hazardous Material Response.	293
407 - Hostage and Barricade Incidents.	296
408 - Response to Bomb Calls.	301
409 - Involuntary Commitments.	306
410 - Citation Releases.	309
411 - Rapid Response and Deployment.	311
412 - Police Escorts.	314
413 - Immigration Violations.	316
414 - Emergency Utility Service.	320
415 - Aircraft Accidents.	321
416 - Field Training Officer Program.	325
417 - Obtaining Air Support.	328
418 - Contacts and Temporary Detentions.	329
419 - Criminal Organizations.	333
420 - Watch Commanders.	337
421 - Mobile Audio Video.	339
422 - Mobile Data Terminal Use.	346

South Salt Lake Police Department

South Salt Lake PD Policy Manual

423 - Portable Audio/Video Recorders.	348
424 - Bicycle Patrol Unit.	354
425 - Foot Pursuits.	358
426 - Burglary/Intrusion Alarm Response.	363
427 - Juvenile Offenders, Contact, Interviews, Interrogation.	365
428 - Automated License Plate Readers (ALPRs).	369
429 - Unusual Occurrence and Planning and Review.	372
430 - Homeless Persons.	381
431 - Legal Process Service and Civil Standby's.	384
432 - Removal of Patrons from Inn's or Motels.	388
433 - Civil Disputes.	390
434 - Public Recording of Law Enforcement Activity.	393
435 - Crisis Intervention Incidents.	396
436 - Medical Aid and Response.	401
437 - First Amendment Assemblies.	406
438 - Suspicious Activity Reporting.	412
439 - School Resource Officers.	414
440 - Body-Worn Cameras.	416
 Chapter 5 - Traffic Operations.	 425
500 - Traffic.	426
501 - Traffic Collisions.	430
502 - Vehicle Towing.	435
503 - Impaired Driving.	439
504 - Traffic Citations.	445
505 - Disabled Vehicles.	447
506 - CHECKPOINTS.	448
507 - Motorcycle Officer Program.	450
 Chapter 6 - Investigation Operations.	 458
600 - Investigation and Prosecution.	459
601 - Detective Availability.	464
602 - Sexual Assault Investigations.	465
603 - Asset Forfeiture.	471
604 - Informants.	479
605 - Accountability and Case Management.	485
606 - Eyewitness Identification.	487
607 - Investigative Task Forces.	491
608 - Brady Material Disclosure.	492
609 - Investigative Polygraphs.	495
610 - Pawn Shop Holds.	496
611 - Sensitive Complaint Processing.	498
612 - Special Operations Procedures.	501
613 - De-Confliction of Activity or Event.	508
614 - Operations Planning and Deconfliction.	511
615 - Warrant Service.	515
616 - Investigative Genetic Genealogy.	520

South Salt Lake Police Department

South Salt Lake PD Policy Manual

617 - Facial Recognition Technology Use.	524
Chapter 7 - Equipment.	531
700 - Department Owned and Personal Property.	532
701 - Information Technology Use.	534
702 - Personal Communication Devices.	538
703 - Vehicle Maintenance.	542
704 - Vehicle Use.	545
705 - High Visibility Reflective Vests.	549
706 - Uniform Requirements and Components.	550
707 - Cash Handling, Security and Management.	560
Chapter 8 - Support Services.	562
800 - Crime Analysis.	563
801 - Property and Evidence.	567
802 - Records Section.	580
803 - Records Management: Access Control, GRAMA request, Data Reporting, Arrest & Warrant Records.	584
804 - Restoration of Firearm Serial Numbers.	592
805 - Records Maintenance and Release.	594
806 - Protected Information.	599
807 - Computers and Digital Evidence.	604
808 - Cash Control of Investigative Funds, Petty Cash, Receipts.	608
809 - Multi-Jurisdictional Communications Agreement.	612
810 - Pharmaceutical Drug Collection Program.	617
811 - Victim Advocates.	619
813 - CJIS Access, Maintenance, and Security.	627
Chapter 9 - Custody.	632
900 - Temporary Custody of Adults.	633
901 - Arrest With or Without a Warrant.	641
902 - Alternative to Arrest.	647
903 - Temporary Detention by Private Persons.	650
904 - Arrest or Detention of Foreign Nationals.	652
905 - Temporary Custody of Juveniles.	656
906 - Custodial Searches.	663
907 - Prison Rape Elimination.	675
908 - Transporting Persons in Custody.	685
Chapter 10 - Personnel.	689
1000 - RECRUITMENT, SELECTION and STANDARDS.	690
1001 - PROMOTIONS AND SPECIALTY ASSIGNMENTS.	695
1002 - Reporting of Arrests, Convictions, and Court Orders.	702
1003 - Drug- and Alcohol-Free Workplace.	704
1004 - Sick Leave.	707
1005 - Communicable Diseases.	709
1006 - Smoking and Tobacco Use.	714

South Salt Lake Police Department

South Salt Lake PD Policy Manual

1007 - Personnel Complaints.	715
1008 - Seat Belts.	726
1009 - Body Armor.	728
1010 - Personnel Records.	730
1011 - Employee/Supervisor Specialty Assignments and Rotations.	734
1012 - Commendations and Awards.	736
1013 - Fitness for Duty.	738
1014 - Meal Periods and Breaks.	741
1015 - Lactation Breaks.	742
1016 - Payroll Records.	744
1017 - Overtime Compensation Requests.	745
1018 - Outside Employment.	749
1019 - Occupational Disease and Work-Related Injury and Death Reporting.	753
1020 - Personal Appearance Standards.	755
1021 - Uniform Regulations.	757
1022 - Nepotism and Conflicting Relationships.	763
1023 - Department Badges.	766
1024 - Temporary Modified-Duty Assignments.	768
1025 - Training and Professional Standards Unit.	773
1026 - Speech, Expression, and Social Networking.	784
1027 - POLICE OFFICER II - PROMOTIONAL CAREER ENHANCEMENT.	789
1028 - Anti-Retaliation.	791
1029 - Workplace Violence.	794
1030 - Wellness Program.	796
1031 - Line-of-Duty Deaths.	801
Attachments.	812
POII Career Enhancement August 2023 Application Form.pdf.	813
Private Persons Temporary Detention Form .pdf.	814
axon_onepager_taserengeryweaponcomparison_17x11_04a-digital.pdf.	815
GSD-SSL SRO Interlocal Agreement 7.29.24 (1).pdf.	816
CJIS Security Policy_v5-8_20190601.pdf.	817
Utah 41-6a-1803 effective May 2024.pdf.	818
Outside Employment Form.pdf.	819
Light Duty Form.pdf.	820

Chapter 1 - Law Enforcement Role and Authority

Law Enforcement Authority

100.1 PURPOSE AND SCOPE

The purpose of this policy is to affirm the authority of the members of the South Salt Lake Police Department to perform their functions based on established legal authority.

100.2 POLICY

It is the policy of the South Salt Lake Police Department to limit its members to only exercise the authority granted to them by law.

While this department recognizes the power of peace officers to make arrests and take other enforcement action, officers are encouraged to use sound discretion in the enforcement of the law. The department does not tolerate abuse of law enforcement authority.

100.2.1 PROHIBITION OF QUOTAS

The South Salt Lake City Police Department shall not establish a minimum requirement or minimum standard regarding the number or percentage or citations or arrests made by its members. This does not prohibit the Department from including a member's engagement with the community or enforcement activity as part of an overall determination of the member's performance (Utah Code 77-7-27)

100.3 PEACE OFFICER POWERS

Sworn members of the Department shall be considered peace officers pursuant to Utah Code 53-13-102 and Utah Code 53-13-103.

100.3.1 ARREST AUTHORITY WITHIN THE JURISDICTION OF THE SOUTH SALT LAKE CITY

The arrest authority within the jurisdiction of the South Salt Lake Police Department includes:

- (a) In compliance with an arrest warrant.
- (b) Without a warrant (Utah Code 77-7-2):
 - (a) For a public offense committed or attempted in the presence of an officer.
 - (b) When an officer has reasonable cause to believe that a felony or class A misdemeanor has been committed.
 - (c) When an officer has reasonable cause to believe that a public offense has been committed and the person to be arrested may flee or conceal him/herself to avoid arrest, destroy or conceal evidence or injure another person or damage property.
- (c) Without a warrant when there is reasonable cause to believe that the person has committed theft (Utah Code 77-7-13).
- (d) Without a warrant when an officer has probable cause to believe that a person is driving under the influence in violation of Utah Code 41-6a-502 (Utah Code 41-6a-508).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Law Enforcement Authority

100.3.2 ARREST AUTHORITY OUTSIDE THE JURISDICTION OF THE SOUTH SALT LAKE CITY

The arrest authority of officers outside the jurisdiction of the South Salt Lake Police Department includes (Utah Code 77-9-3):

- (a) When the officer is in fresh pursuit of an offender for the purpose of arresting and holding the person in custody or returning the person to the jurisdiction where the offense occurred.
- (b) When a public offense has been committed in the presence of the officer.
- (c) When the officer is participating in an investigation of criminal activity which originated in the jurisdiction of the South Salt Lake Police Department in cooperation with the local law enforcement authority.
- (d) When the officer is called to assist officers in another jurisdiction.

Officers should, when practicable, notify and receive approval from the local law enforcement authority prior to taking enforcement action.

100.4 CONSTITUTIONAL REQUIREMENTS

All members shall observe and comply with every person's clearly established rights under the United States and Utah Constitutions.

100.4.1 LIMITS OF AUTHORITY

- (a) It is the duty of each of the sworn personnel in the department to enforce all laws and ordinances in the City of South Salt Lake.
- (b) The officers authority will be utilized within the limits of the law, city ordinance, state and federal constitutions, and the standards adopted by this department.
- (c) Full-time peace officers have peace officer authority 24 hours a day, 7 days a week.
- (d) Reserve officers shall have peace officer authority only while on duty and functioning in an official capacity as a reserve officer for the City of South Salt Lake.
- (e) Crossing guards shall have no authority to arrest or enforce any law.

100.4.2 LEGAL AUTHORITY TO CARRY FIREARMS

Peace officers are authorized to carry firearms under the Constitution of the State of Utah, Article 1, section 6 and UCA '76-10-523.

100.4.3 GEOGRAPHICAL JURISDICTION

In the delivery of emergency law enforcement services there can be no boundaries. Whenever an emergency need is identified or whenever fellow law enforcement officers are in need of assistance, geographical boundaries should not hinder an officer from answering the call or honoring the request. However, the day-to-day tasks of providing police services and the overall exercise of police authority will normally be limited to those areas within the corporate limits of South Salt Lake City.

- (a) Peace officers have statewide peace officer authority. UCA 77-1a-1(2).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Law Enforcement Authority

- (b) Any peace officer duly authorized by any governmental entity of this state may exercise a peace officer's authority beyond the limits of such officer's normal jurisdiction where the offense was committed when:
 - 1. A public offense is committed in such officer's presence.
 - 2. Participating in an investigation of criminal activity which originated in such officer's normal jurisdiction in cooperation with the local authority.
 - 3. Called to assist peace officers of another jurisdiction.
 - 4. Serving as a member of a law enforcement task force.
- (c) Any peace officer, prior to taking such authorized action, shall notify and receive approval of the local law enforcement authority, or if such prior contact is not reasonably possible, notify the local law enforcement authority as soon as reasonably possible.
- (d) Unless specifically requested to aid a police officer of another jurisdiction or otherwise as provided for by law, no legal responsibility for a police officer's action provided herein, shall attach to the local law enforcement authority. UCA 77-9-3.

100.5 INTERSTATE PEACE OFFICER POWERS

Peace officer powers may be extended to other states:

- (a) As applicable under interstate compacts, memorandums of understanding or mutual aid agreements in compliance with the laws of each state.
- (b) When an officer enters another state in fresh pursuit:
 - 1. In Colorado, to arrest the person for a crime committed in Utah (CRS § 16-3-104).
 - 2. In Arizona, Idaho, Nevada and New Mexico, to arrest the person for committing a felony in Utah (ARS § 13-3832; Idaho Code 19-701; NRS 171.158; NMSA § 31-2-1).
- (c) When an interstate compact exists with the state of Wyoming that permits an officer to pursue and arrest an offender who has fled Utah (Wyo. Stat. § 7-3-103).

Whenever an officer makes an arrest in another state, the officer shall take the offender to a magistrate or other proper judicial official in the county where the arrest occurred as soon as practicable (ARS § 13-3833; CRS § 16-3-104; Idaho Code 19-702; NRS 171.158; NMSA § 31-2-2 (New Mexico)).

100.6 ARREST REVIEWS

Before any booking of an arrested person into jail or any official detention facility, a documented arrest review shall occur by the arresting officer and supervisor. If, at any time during an arrest, force is used on an individual, a sergeant or other sworn supervisor will be called to the scene to review the arrest. This policy does not preclude a supervisor from responding to other calls or reviewing arrests in cases not involving force. If any individual request to speak to supervisor, the officer or employee must notify the duty supervisor as soon as practical.

Chief Executive Officer

101.1 PURPOSE AND SCOPE

Utah Code 53-6-205 mandates that all sworn officers employed after January 1, 1985 successfully complete a Utah POST Council certified academy or successfully pass a state certification examination pursuant to Utah Code 53-6-206, and obtain POST certification, prior to being permitted to exercise peace officer powers.

101.1.1 CHIEF OF POLICE REQUIREMENTS

It is recommended that a candidate for Chief of Police of the Department should, as a condition of continued employment:

- (a) Be an individual of recognized executive and administrative capacity.
- (b) Be selected solely with regard to their qualifications and fitness to discharge the duties of the office.
- (c) Be of high moral character.
- (d) Be of good standing in their community of residence.

Policy Manual

102.1 PURPOSE AND SCOPE

The manual of the South Salt Lake Police Department is hereby established and shall be referred to as the Policy Manual or the manual. The manual is a statement of the current policies, rules and guidelines of this department. All members are to conform to the provisions of this manual.

All prior and existing manuals, orders and regulations that are in conflict with this manual are rescinded, except to the extent that portions of existing manuals, procedures, orders and other regulations that have not been included herein shall remain in effect, provided that they do not conflict with the provisions of this manual.

102.2 POLICY

Except where otherwise expressly stated, the provisions of this manual shall be considered as guidelines. It is recognized that the work of law enforcement is not always predictable and circumstances may arise which warrant departure from these guidelines. It is the intent of this manual to be viewed from an objective standard, taking into consideration the sound discretion entrusted to members of this department under the circumstances reasonably available at the time of any incident.

102.2.1 DISCLAIMER

The provisions contained in the Policy Manual are not intended to create an employment contract nor any employment rights or entitlements. The policies contained within this manual are for the internal use of the South Salt Lake Police Department and shall not be construed to create a higher standard or duty of care for civil or criminal liability against the City, its officials or members. Violations of any provision of any policy contained within this manual shall only form the basis for department administrative action, training or discipline. The South Salt Lake Police Department reserves the right to revise any policy content, in whole or in part.

102.2.2 COMMAND STAFF

Command Staff shall consist of the following:

- Chief of Police
- Deputy Chief of Police
- Division Commanders

The Command Staff shall review all recommendations regarding proposed changes to the manual at staff meetings.

102.3 AUTHORITY

The Chief of Police shall be considered the ultimate authority for the content and adoption of the provisions of this manual and shall ensure compliance with all applicable federal, state and local laws. The Chief of Police or the authorized designee is authorized to issue General Orders, which

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Policy Manual

shall modify those provisions of the manual to which they pertain. General Orders shall remain in effect until such time as they may be permanently incorporated into the manual.

102.4 DEFINITIONS

The following words and terms shall have these assigned meanings throughout the Policy Manual, unless it is apparent from the content that they have a different meaning:

Adult - Any person 18 years of age or older.

CFR - Code of Federal Regulations.

City - The City of South Salt Lake.

Non-sworn - Employees and volunteers who are not sworn peace officers.

Department/SSLPD - The South Salt Lake Police Department.

DMV - The Department of Motor Vehicles.

Employee/personnel - Any person employed by the Department.

Juvenile - Any person under the age of 18-years.

Manual - The South Salt Lake Police Department Policy Manual.

May - Indicates a permissive, discretionary or conditional action.

Member - Any person employed or appointed by the South Salt Lake Police Department, including full-time sworn officers, reserve officers, non-sworn employees and volunteers.

Officer - Those employees, regardless of rank, who are sworn peace officer employees of the South Salt Lake Police Department.

On-duty - A member's status during the period when he/she is actually engaged in the performance of his/her assigned duties.

Order - A written or verbal instruction issued by a superior.

POST - The Utah Peace Officer Standards and Training Division.

Rank - The title of the classification held by an officer.

Shall or will - Indicates a mandatory action.

Should - Indicates a generally required or expected action, absent a rational basis for failing to conform.

Supervisor - A person in a position of authority regarding hiring, transfer, suspension, promotion, discharge, assignment, reward or discipline of other department members, directing the work of other members or having the authority to adjust grievances. The supervisory exercise of authority may not be merely routine or clerical in nature but requires the use of independent judgment.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Policy Manual

The term "supervisor" may also include any person (e.g., officer-in-charge, lead or senior worker) given responsibility for the direction of the work of others without regard to a formal job title, rank or compensation.

When there is only one department member on-duty, that person may also be the supervisor, except when circumstances reasonably require the notification or involvement of the member's off-duty supervisor or an on-call supervisor.

UAC - Utah Administrative Code (Example: UAC R728-503-10).

USC - United States Code.

102.5 ISSUING THE POLICY MANUAL

An electronic version of the Policy Manual will be made available to all members on the department network for viewing and printing. No changes shall be made to the manual without authorization from the Chief of Police or the authorized designee.

Each member shall acknowledge that he/she has been provided access to, and has had the opportunity to review the Policy Manual and General Orders. Members shall seek clarification as needed from an appropriate supervisor for any provisions that they do not fully understand.

102.6 PERIODIC REVIEW OF THE POLICY MANUAL

The Chief of Police will ensure that the Policy Manual is periodically reviewed and updated as necessary.

102.7 REVISIONS TO POLICIES

All revisions to the Policy Manual will be provided to each member on or before the date the policy becomes effective. Each member will be required to acknowledge that he/she has reviewed the revisions and shall seek clarification from an appropriate supervisor as needed.

Members are responsible for keeping abreast of all Policy Manual revisions.

Each Division Commander will ensure that members under his/her command are aware of any Policy Manual revision.

All department members suggesting revision of the contents of the Policy Manual shall forward their written suggestions to their Division Commanders, who will consider the recommendations and forward them to the command staff as appropriate.

Professional Standards and Conduct

103.1 PURPOSE AND SCOPE

The Professional Standards and Conduct Section shall be considered as standing orders governing the actions of all employees of the South Salt Lake City Police Department in the performance of their duties.

103.1.1 PROCEDURE

All employees of the South Salt Lake City Police Department shall review the Professional Standards and Conduct Section during their field training process.

All employees shall read and familiarize themselves with the contents of the manual

103.2 OBLIGATION TO DEPARTMENT GOALS AND OBJECTIVES

Supervisory and management personnel shall be familiar with the mission, and vision statements and integrate into their daily activities, the goals and objectives of the Department.

Officers shall preserve the public peace, involve the community in problem solving whenever possible, detect, and arrest offenders, prevent crime, protect life and property, and enforce the ordinances and statutes of the City of South Salt Lake, the State of Utah, and the United States of America.

Non-sworn employees, although not personally responsible for the enforcement of the law, shall provide vital support for the Department's basic mission.

103.3 INSUBORDINATION AND INTEMPERATE BEHAVIOR

Employees shall obey, in a timely manner, any lawful directives of a supervisor

Employees shall not show, by statement or deed disrespect to a supervisor

Employees shall not show, by statement or deed disobedience to authority

Employees shall not be obligated to obey any directive which they know or should reasonably know would require them to commit any illegal act. If in doubt as to the legality of a directive, employees shall request the issuing supervisor to clarify the directive or shall request to confer with higher authority.

103.4 IDENTIFICATION

Employees shall furnish their names and identification number to any person requesting that information when they are on duty or while holding themselves out as having official capacities, except when the withholding of such information is necessary for the performance of the police duties or is authorized by the employee's supervisor.

103.5 DERELICTION OF DUTY

Dereliction of duty, on the part of any employee, is cause for disciplinary action. The following acts or omission shall constitute dereliction of duty:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Professional Standards and Conduct

1. Failure to obey a lawful order(s) or willful or repeated violations of any rule, regulation or policy of the department.
2. Employees shall submit all necessary reports on time and in accordance with established department procedures. Reports submitted by employees shall be truthful and complete, and no employees shall knowingly enter or cause to be entered any inaccurate, false or improper information.
3. Any Employee absent without authorized leave. This rule includes failure to be at the time and place of duty or leaving a place of duty or assignment without authorization.
4. Cowardice or failure to support fellow officers or perform police duties because of fear.
5. Sleeping while on duty.
6. Falsely reporting themselves ill or injured, or to otherwise deceive or attempt to deceive the department as to the condition of their health. Employees, when reporting off sick for any reason other than emergency, shall notify their respective on-duty supervisor at least one (1) hour prior to the employees scheduled hours of duty. This notification shall take place on a daily or as needed basis unless excused for doing so by the employee's supervisor.
7. Purposefully or by lack of proper planning fails to complete required training.
8. Devoting on-duty time and attention to non-department business Any exceptions to this rule shall be only with the approval of the Chief of Police.
9. Using abusive, insulting or indecent language toward or about a supervisor, peer, citizen, etc.
10. Displaying reluctance to properly perform assigned duties or acting in a manner tending to bring discredit upon him/herself or a department, or failing to assume responsibility or exercise diligence and interest in pursuit of duties, or displaying a lack of energy of such character as to amount to incompetence
11. Failure of a supervisor to immediately take action when a violation of this sections comes to his/her attention.
12. Use of tobacco, alcohol and/controlled substance in violation of these standards.

103.6 AVAILABILITY OF PERSONAL INFORMATION

Each employee shall keep the department informed of his/her current address and telephone.

Each employee shall report any changes in address or telephone number within twenty-four (24) hours to his/her Field Commander, Division Commander and Administrative Assistant.

Address and telephone numbers of employees shall be kept confidential and released only by direction of the Chief of Police or his/her designee.

103.7 CONDUCT UNBECOMING A POLICE EMPLOYEE

It is important for police officers and police employees to maintain the respect and trust of the community as well as the trust and respect of their fellow officers and other department employees. Employees shall be truthful in deeds and scope of employment operations. It is imperative that

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Professional Standards and Conduct

an officers/employee's conduct both on-duty and off-duty not negatively affect the mission of the South Salt Lake Police Department or negatively impact the general positive reputation of this department. Officers/employees shall not engage in any conduct on-duty or off-duty, which brings discredit or embarrassment to the employee and/or the department. An officers/employee's on-duty and off-duty conduct should not negatively affect the morale and/or day-to-day operations of the department. Example would be but are not limited to: bigotry, dishonesty, fighting, mishandling of property belonging to the department or others, verbal tantrums.

103.8 PATRIOTIC COURTESY

1. On all occasion, sworn employees of this department while in uniform shall salute the National colors and the playing of the National Anthem with a hand salute unless officers are performing police duty requiring immediate attention.
2. Employees of this department who are not in uniform shall render the National Colors and National Anthem the honors and courtesies customarily afforded them.

Oath of Office

104.1 PURPOSE AND SCOPE

Officers of the Department are sworn to uphold the federal and state constitutions and to enforce federal, state and local laws.

104.2 POLICY

It is the policy of the South Salt Lake Police Department that, when appropriate, department members affirm the oath of their office as an expression of commitment to the constitutional rights of those served by the Department and the dedication of its members to their duties.

104.3 OATH OF OFFICE

All department members, when appropriate, shall take and subscribe to the oaths or affirmations applicable to their positions (Utah Constitution Article IV § 10).

If a member is opposed to taking an oath, he/she shall be permitted to substitute the word "affirm" for the word "swear."

104.3.1 NEWLY APPOINTED OFFICERS_DEPUTIES

Newly appointed officers shall take and abide by the oath of office before assuming sworn status.

104.4 SOUTH SALT LAKE POLICE OFFICER'S OATH OF OFFICE STATE OF UTAH)

: ss

COUNTY OF SALT LAKE)

I do solemnly affirm that I will conform to the high standards set forth in the LAW ENFORCEMENT CODE OF ETHICS and POLICE DEPARTMENT VALUE STATEMENT, and that I will support and obey; in word and deed, the POLICE DEPARTMENT CODE OF CONDUCT and affirmatively promote the mission outlined in the POLICE DEPARTMENT MISSION STATEMENT.

I do solemnly affirm that I will support, obey, and defend the CONSTITUTION OF THE UNITED STATES and the CONSTITUTION OF THE STATE OF UTAH, and that I will discharge the duties of my office with fidelity.

(Sign Here) _____

(Office) Police Officer

Subscribed and sworn to before me this day of

City Recorder

City of South Salt Lake, Utah

OATH OF OFFICE

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Oath of Office

OF

As

Police Officer

Filed the

_____ Clerk or Recorder

By _____ Chief of Police

104.5 MAINTENANCE OF RECORDS

The oath of office shall be filed as prescribed by law (Utah Code 52-1-2 et seq.).

Constitutional Safeguards - Investigations

105.1 PURPOSE AND SCOPE

It is the policy of South Salt Lake Police Department to respect and protect the individual constitutional rights of all persons and to take firm and decisive action against any sworn officer who, in the course of duty, deliberately and knowingly, without justification, violates the individual constitutional rights of any person.

- (a) Certain individual constitutional rights are viewed as being particularly susceptible to abuse during the conduct of law enforcement activities. Among these are constitutional prohibitions against:
 - 1. Unreasonable searches and seizures.
 - 2. Self incrimination.
 - 3. Deprivation of life or liberty without due process.
 - 4. Criminal proceedings without assistance of counsel.
- (b) Officers must be sensitive to these constitutional issues and remain alert for case law interpretations and statutory augmentation arising out of the above topics. Some restrictions and considerations that apply are:
 - 1. Absent exigent circumstances, probable cause, or consent to search, search warrants will be obtained prior to searches.
 - 2. Use of only necessary and proper physical force.
 - 3. Ensuring the physical safety of persons in custody.
 - 4. Arrests are based on personal observation, probable cause, or as directed by a warrant.
 - 5. Persons who are being interviewed will be advised of their rights per the Miranda Warning, if in the course of the interview they are suspected of criminal activity or the officer believes they may make self incriminating statements.
 - 6. Persons in custody who are being questioned will be advised of their rights per the Miranda Warning.
 - 7. Confessions and admissions will be voluntary.
 - 8. Allowing the arrestees attorney to have access to his/her client in custody so as to not deprive the arrestee of counsel.
- (c) Intentional or careless denial of a person's constitutional rights may result in criminal or civil sanctions against those involved, as well as disciplinary action against department employees.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Constitutional Safeguards - Investigations

105.1.1 ELECTRONIC RECORDING OF CUSTODIAL INTERVIEWS

The South Salt Lake Police Department will adopt the following practices for electronic recording of custodial interviews. The state prosecutors, the Utah Attorney General's office and the Utah Chiefs of Police Association have implemented the attached statement of best practices regarding the recording of interrogations. With this statement, we are compatible with our prosecutors who must represent our actions in court.

105.1.2 POLICY

- (a) Any custodial interrogation of a person who is in a fixed place of detention and who, at the time of the interrogation, is suspected of having committed any violent felony offense, as defined in Utah Code Ann. §76-3-203.5(1)(c)(i), should be electronically recorded in its entirety.
- (b) Any custodial interrogation of a person who is not in a fixed place of detention and who, at the time of the interrogation, is suspected of having committed any violent felony offense, as defined in Utah Code Ann. §76-3-203.5(1)(c)(i), should, where practicable, be electronically recorded in its entirety.
- (c) The interrogating entity should not destroy or alter any electronic recording made of a custodial interrogation until the time that a conviction for any offense relating to the interrogation is final and all direct and collateral appeals are exhausted or the prosecution for that offense is barred by law. To facilitate storage and protection of the record during the time period specified above, the interrogating entity may make true, accurate, and complete copies of the electronic recording.
- (d) The guidelines for electronic recording of a custodial interrogation are not applicable if:
 - 1. The suspect refuses to speak to law enforcement if the interrogation is electronically recorded. Such refusal should be documented either by electronic recording demonstrating such refusal, or through a written statement signed by the suspect.
 - 2. Access to recording equipment required to electronically record an interrogation is not reasonably available during the period of time that the suspect is lawfully detained.
 - 3. The equipment malfunctions and replacement equipment is not reasonably available.
 - 4. The law enforcement officers, in good faith, fail to record the custodial interrogation because the officers inadvertently fail to operate the recording equipment properly, or without the officer's knowledge the recording equipment malfunctions or stops operating.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Constitutional Safeguards - Investigations

5. The law enforcement officers conducting the custodial interrogation reasonably believe that the crime of which the person is suspected is not among those listed in Utah Code Ann §76-3-203.5(1)(c)(i).
 6. Exigent circumstances make electronic recording impossible or impractical.
- (e) Definitions applicable to this best practices statement are as follows:
1. **Custodial interrogation** - means express questioning or its functional equivalent that is conducted by a law enforcement officer from the time the suspect is, or should be, informed of his or her "Miranda" rights, until the time that the questioning ends. It does not include questions put by law enforcement personnel, and the person's responsive statements, which are part of a routine processing or booking of the person.
 2. **Electronic recording** - refers to either audio recording or combined audio and video recording. The latter is recommended. Law enforcement officers are encouraged, if videotaping, to position the camera to capture the suspects face.
 3. **Fixed place of detention** - means a jail, a police or sheriff's station, a holding cell, or a correctional or detention facility.
 4. **Suspect** - a person who enforcement officers have reasonable cause, at the time of the interrogation, to believe committed a violent felony.
- (f) Law enforcement officers should continue to prepare written summaries of custodial questioning, and continue to obtain written statements from suspects. [NOTE: This document provides recommendations for electronic recording of custodial questioning. No document can address all the circumstances or exigencies which officers may encounter, and this model is not intended to be a comprehensive treatment of all the factors involved in criminal investigations. While it is a general guide outlining methods for custodial questioning, the recommendations are intended to be used as guidelines, and are not intended to create any substantive or procedural rights.]

Federal Law Enforcement or National Guard Assistance

106.1 PURPOSE AND SCOPE

Federal assistance is requested through the Office of the Federal Emergency Management Agency (FEMA).

- (a) State assistance, including assistance from the National Guard, is requested through the office of the Governor.
- (b) The Mayor or Mayor's designee shall, in the absence of the Mayor, request emergency mutual aid from the state or federal government.

Chapter 2 - Organization and Administration

Staffing Levels

200.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines to ensure that proper supervision is available to meet the needs of the [Department/Office] and members throughout all Divisions.

200.2 POLICY

The South Salt Lake Police Department will ensure that proper supervision is available to meet the needs of its members and to achieve the goals of the [Department/Office]. The needs of its members should be balanced with the needs of the [Department/Office] for flexibility and discretion in assigning members to meet supervisory needs. While balance is desirable, the paramount concern is to meet the needs of the [Department/Office].

200.3 MINIMUM SUPERVISION STAFFING LEVELS

Minimum staffing levels should be established by the Division Commanders for each Division and work group. The supervision staffing levels should support proper supervision, span of control, and activity levels to meet the needs of members and the goals of the [Department/Office]. Each patrol platoon shifts should be at a minimum of three officers and one sergeant.

200.3.1 SHIFTS AND SCHEDULES

Patrol works a rotating Platoon schedule that alternates working weekends. Patrol is on 10 hour shifts; dayshift 0600-1600 hours, afternoon 1400-0000hours, graves 2100-0700 hours there are some variations due to call volume. Detectives work 10 hour shifts. Community Resource Officers work 10 hour shifts, Homeless Resource Officers work 10 hour shifts with weekend 12 hour shifts., School Resource Officer and Youth Resource Officer will work to accommodate the needs of the assigned schools. Administration is on 8 hour shifts. The shift rotation is a four month cycle. Shifts or rotations maybe changed at anytime to meet the needs of the police department at the direction of the Chief of Police.

Organizational Structure and Responsibility

201.1 PURPOSE AND SCOPE

This policy establishes the organizational structure of the [Department/Office] and defines general responsibilities of [department/office] members.

201.1.1 OFFICE OF THE CHIEF OF POLICE

The Chief of Police is responsible for administering and managing the South Salt Lake Police Department, and supervises either directly or indirectly all department personnel, establishes department policies, prepares the police department budget, approves department expenditures, and implements city policy directives as ordered by the Mayor. The Chief of Police oversees the Deputy Chief of Police,, and the Executive Assistant. The Executive Assistant oversees Records.

201.2 DIVISIONS

There are four Divisions in the Police Department as follows:

- Patrol
- Investigations
- Homeless Resource
- Professional Standard/Community Resource

The Patrol Division will be overseen by two Lieutenants.

The Investigations Division will be overseen by a Lieutenant.

The Professional Standards/Community Resources Division will be overseen by a Lieutenant.

The Homeless Resource Division will be overseen by a Lieutenant.

The Chief of Police and Deputy Chief of Police are responsible for strategic decisions centered on overall goals and objectives as well as long range direction of the department.

201.2.1 PATROL DIVISION

The Patrol Division is commanded by two Lieutenants who report directly to the Deputy Chief of Police. The Patrol Division is comprised of six (6) uniformed patrol squads. Each squad is overseen by a Sergeant. Each Sergeant reports to a Lieutenant. Each assigned Lieutenant, whose primary responsibility is to provide general management, direction, and oversight for the Patrol Division. The Patrol Division consist of uniformed patrol and special operations.

- (a) In addition to uniformed patrol, other units functioning within the Patrol Division include: Traffic, Police Service Dogs, Major Accident Investigations, Public Oder, S.W.A.T.,,, Bike Patrol and the Honor Guard.
- (b) The Patrol Division shall be responsible to cooperate with the community in protecting life, property, preserving public peace, preventing crime, responding to calls for service, providing traffic enforcement and control as well as providing other community services.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Organizational Structure and Responsibility

201.2.2 INVESTIGATIONS DIVISION

The Investigations Division is commanded by a Lieutenant who reports directly to the Deputy Chief of Police. The Investigation Division is comprised of two units. Each unit is overseen by a Sergeant. Both Sergeants report to the Investigations Division Lieutenant. The assigned Lieutenant, whose primary responsibility is to provide general management, direction and oversight for the Investigation Division.

- (a) The Investigations Division is comprised of detectives who report to a Sergeant. The Sergeant reports to the Lieutenant. Civilian staff reports to the Lieutenant.
- (b) The Investigations Division includes General Investigations, Victim Advocates, Evidence, Crime Scene Investigations, and Task Force assignments.
- (c) The Investigations Division is responsible for investigations as directed by the Sergeant(s) and/or Lieutenant. In addition, the Investigations Division shall be responsible to cooperate with the community in protecting life, property, preserving public peace, and preventing crime through the investigation of criminal activity as well as providing other community services.

201.2.3 PROFESSIONAL STANDARDS/COMMUNITY RESOURCE DIVISION

The Professional Standards/Community Resource Division is commanded by a Lieutenant who reports directly to the Deputy Chief of Police. The assigned Lieutenant, whose primary responsibility is to provide general management, direction, and oversight of recruitment, retention, training, liaison to the civil review board, liaison with the Granite School District, Crime Analysts, training sergeant and school resource sergeant.

- (a) The Community Resources Unit (CRU) is managed and supervised by the Professional Standards Sergeant, who reports to the Professional Standards/Community Resource Division Lieutenant who reports to the Deputy Chief of Police.
- (b) The School Resource Officer assigned to Granite Park Jr High, the Youth Resource Officer, and Crossing Guards are supervised by the School Resource Sergeant, who reports to the Professional Standards/Community Resource Division Lieutenant who reports directly to the Deputy Chief.
- (c) The Community Resource Unit will be responsible to cooperate with the community in protecting life, property, preserving public peace and crime prevention. The CRU will partnership with the community using Crime Free Housing, Business Watch, Neighborhood Watch and other assigned community events.
- (d) The Crime Analysts will report directly to the Professional Standards/Community Resource Lieutenant for assignment and scheduling.

201.2.4 ROLES AND RESPONSIBILITIES

In the event that the Chief of Police or any acting Chief of Police is required to be absent from the city and cannot effectively perform the duties of the position, this written directive will serve as a written order to assign the next ranking officer in order of succession as the Acting Chief. The ranking officer will assume the duties and responsibilities of the Chief of Police during the Chief's absence.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Organizational Structure and Responsibility

- (a) Should the Chief of Police become incapacitated through illness, death, or absence or for any other reason, the first ranking officer in the order of succession will assume command of the department as Acting Chief of Police. In the event the Acting Chief of Police becomes incapacitated or is absent from the city, the next ranking officer listed in the order of succession will assume command of the department.
- (b) The hierarchal succession of command for the South Salt Lake City Police Department, under exceptional situations, shall be as follows:
 - 1. The Chief of Police.
 - 2. Deputy Chief of Police.
 - 3. Investigative Lieutenant
 - 4. Professional Standards Lieutenant
 - 5. Homeless Resource Lieutenant
 - 6. Watch Commander/Duty Lieutenant by seniority
 - 7. The remaining order of succession will be determined by time in rank seniority in the rank of sergeant then if need be police officer..
- (c) Normal day to day operations:
 - 1. Lieutenants shall be of equal authority in respect to their assigned responsibilities.
 - 2. Watch Commanders (Lieutenants) will also act as the primary administrative supervisors for each platoon they are assigned.
 - 3. Patrol sergeants shall be the operational supervisors for officers working their shifts.
 - 4. The Investigations Lieutenant will also act as the primary administrative supervisor for those investigators whose assignments are under his/her direction.
 - 5. Investigations sergeants shall be the operational supervisors for investigators working their shifts.
 - 6. Administrative functions will include the approval of time off, first reports, citations, etc. Operational functions will include deployment of personnel, and other day-to-day duties, which require an immediate response or police action.
 - 7. From time to time, officers from other divisions may carry out patrol assignments, or in the case of traffic officers, may be working in the field without their immediate supervisor. These officers should be considered under the operational control of the shift supervisor on duty.
 - 8. The on duty shift supervisor will act as the Police Service Dog Officer's supervisor in regards to shift related matters. The assigned Police Service Dog Unit supervisor will handle administrative issues.
- (d) Whenever the department engages in an operation involving more than one division, and/or more than one shift, the overall command of the operation will be assigned to

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Organizational Structure and Responsibility

the supervisor of the division, section, or shift initiating the event, unless otherwise directed by the on-call commander, the Chief of Police or his/her designee.

201.3 COMMAND PROTOCOL

The principles of unity of command ensure efficient supervision and control within the Department. The chain of command of the South Salt Lake Police Department consists of the Chief of Police as the department head. Next in command during the Chief's absence, unless otherwise designated by the Chief of Police, is the Deputy Chief of Police, Lieutenants by seniority, Sergeants by seniority, and Officers by seniority, in that respective order.

- (a) If an officer has responsibilities that fall under the direction of more than one supervisor, the officer is directly accountable to the supervisor related to the particular assignment.
- (b) Each organizational component within the department shall be under the direction of one supervisor.
- (c) The Deputy Chief of Police reports to the Chief of Police.
- (d) Lieutenants report to the Deputy Chief of Police.
- (e) Sergeants report to Lieutenants.
- (f) Officers report to Sergeants.

201.3.1 UNITY OF COMMAND

The principles of unity of command ensure efficient supervision and control within the [Department/Office]. Generally, each employee shall be accountable to one supervisor at any time for a given assignment or responsibility. Except where specifically delegated authority may exist by policy or special assignment (e.g., canine, bicycle patrol), any supervisor may temporarily direct any subordinate if an operational necessity exists.

201.3.2 ORDERS

Members shall respond to and make a good faith and reasonable effort to comply with the lawful order of superior officers and other proper authority.

201.3.3 DELEGATION OF AUTHORITY

The Chief of Police or designee may delegate authority as necessary to meet the needs of the department. Delegated authority shall be commensurate with the individual's responsibilities and assigned position. No person may be delegated to supervise personnel of a higher rank.

- (a) Any person having been delegated authority, to act in an assignment, will make the necessary decisions needed to achieve successful results. To aid in this, the department will assist in the decision making process by providing adequate training and/or clear direction necessary to function in any assignment(s).
- (b) Officers and supervisory/command staff will abide by department standards, laws, and direction in exercising this authority and will keep employees aware of problems and/or results, which occur, per policy.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Organizational Structure and Responsibility

(c) Accountability:

1. It is the expectation of this department that any employee-delegated authority will recognize and accept the need for individual accountability for actions resulting from delegated authority. This accountability extends to any employee-delegated authority that fails to use the responsibility when warranted and/or expected.
2. Therefore, all employees are expected to be aware of department policies, standards, orders, and other related matters as found in city policy, as well as personnel rules and regulations.

201.4 AUTHORITY AND RESPONSIBILITY

Consistent with the principles of sound supervisory practices, all supervisory personnel will be held accountable for the performance of their subordinates. To facilitate this end, training requirements for supervisory personnel are assigned in the job description and job task analysis, and in-service training for supervisors shall address employee career development.

Irrespective of rank, each employee within the organization has clearly articulated duties and responsibilities. Each employee is hereby delegated the authority necessary to effectively execute those responsibilities. Each employee will also be held accountable for the appropriate application of that delegated authority.

201.4.1 SUPERVISORY ACCOUNTABILITY

A. Supervisory personnel are accountable for the performance of the employees operating under their immediate control. Commensurate with this responsibility, the span of control of supervisory personnel will be limited. Division Commanders will assess the spans of control at each organizational level within their divisions and impose limits as indicated by individual supervisory assignments to ensure that current spans of control are not excessive.

201.5 MULTI-YEAR PLAN

The Chief of Police or the authorized designee is responsible for establishing a multi-year plan, which includes:

- Goals and operational objectives.
- Anticipated workloads and population trends.
- Anticipated personnel levels.
- Anticipated capital improvement and equipment needs.

201.6 JOB DESCRIPTIONS

The Administration Division Commander shall ensure that a current job description is maintained for each position in the [Department/Office]. Job descriptions shall include the duties and responsibilities of each position, including entry-level requirements, and be made available to all members.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Organizational Structure and Responsibility

201.7 CIVILIAN NON-SWORN CONSIDERATIONS (PROFESSIONAL SUPPORT STAFF)

Assignments for non-sworn members shall take into consideration that they:

- Shall not be commissioned as officers.
- Shall not be assigned to duties requiring sworn officer status.
- Shall perform the duties described and governed by appropriate policy and receive training in the proper performance of such duties.
- Shall not wear a police uniform.
- Non-sworn personnel will wear a uniform that clearly distinguishable from that of a sworn officer.

Electronic Mail

202.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the proper use and application of the [department/office]'s electronic mail (email) system provided by the [Department/Office].

202.2 POLICY

South Salt Lake Police Department members shall use email in a professional manner in accordance with this policy and current law (e.g., Utah Government Records Access and Management Act).

202.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to emails accessed, transmitted, received, or reviewed on any [department/office] technology system (see the Information Technology Use Policy for additional guidance).

202.4 RESTRICTIONS ON USE OF EMAIL

Messages transmitted over the email system are restricted to official business activities, or shall only contain information that is essential for the accomplishment of business-related tasks or for communications that are directly related to the business, administration, or practices of the [Department/Office].

Sending derogatory, defamatory, obscene, disrespectful, sexually suggestive, harassing, or any other inappropriate messages on the email system is prohibited and may result in discipline.

Email messages addressed to the entire [Department/Office] are only to be used for official business-related items that are of particular interest to all users. In the event that a member has questions about sending a particular email communication, the member should seek prior approval from a supervisor in their chain of command.

It is a violation of this policy to transmit a message under another member's name or email address or to use the password of another to log into the system unless directed to do so by a supervisor. Members are required to log off the network or secure the workstation when the computer is unattended. This added security measure will minimize the potential misuse of an individual's email, name, or password. Any member who believes their password has become known to another person shall change their password immediately.

202.5 EMAIL RECORD MANAGEMENT

Email may, depending upon the individual content, be a public record under the Utah Government Records Access and Management Act (Utah Code 63G-2-201 et seq.) and must be managed in accordance with the established records retention schedule and in compliance with state law.

The Records Officer shall ensure that email messages are retained and recoverable as outlined in the Records Maintenance and Release Policy.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Electronic Mail

202.6 CITY COMPUTER USE POLICY

Police department employees must also adhere to the City of South Salt Lake Computer Use policy. This policy can be found in the city employee personnel manual.

Administrative Communications

203.1 PURPOSE AND SCOPE

Administrative communications of the Department are governed by the following policies.

203.2 PERSONNEL ORDER

Personnel Order may be issued periodically by the Chief of Police or Deputy Chief of Police to announce and document all promotions, transfers, hiring of new personnel, separations, personnel and group commendations, or other changes in status.

203.3 CORRESPONDENCE

In order to ensure that the letterhead and name of the Department are not misused, all external correspondence shall be on Department letterhead. All Department letterhead shall bear the signature element of the Chief of Police. Personnel should use Department letterhead only for official business and with approval of their supervisor.

203.4 COMMUNICATION AND INFORMATION SHARING

The free flow of information in the South Salt Lake City Police Department is aided by a variety of formal and informal reports that are forwarded to the appropriate division, section, or unit. Methods used to promote this free flow of information include:

(a) Definitions:

1. **Briefing** - This is the time period at the beginning of the officer's tour of duty during which information may be exchanged with other departmental units, or investigators may provide patrol officers with leads on major cases. The patrol officers represent resources for the investigators through street contacts on a daily basis. Frequent informal contacts between investigators and patrol officers in the briefing setting are vital to fostering and maintaining open communications channels.
2. **Unit and Section Staff Meetings** - The unit or section will hold meetings according to the unit/sections needs. The unit/section supervisor will decide the frequency of such meetings.
3. **Divisional Staff Meetings** - These meetings, set by the Division Commanders, are to create opportunities for providing information to all of the first-line supervisors within the respective division. Those in attendance represent all sections of the division and provide for the three-way exchange of information relating to the common concerns and problems of the first- line supervisor.
4. **Department Staff Meetings** - These meetings are set by the Chief of Police, or designee, and provide an opportunity to disseminate information to the entire department. Those in attendance represent all sections of the department and

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Administrative Communications

the meeting provides an opportunity for the three-way exchange of information relating to all aspects of the operation and functions of the department.

- (b) There are a variety of police hazards that can be brought to the attention of the police department on a daily basis. The complaints or advisements can come from a variety of sources:
 - 1. Other officers within the agency.
 - 2. Officers from other agencies.
 - 3. Concerned citizens.
 - 4. Other city departments.
 - 5. Victims or potential victims.
 - 6. Other governmental agencies (parole, probation, courts, etc.)
- (c) Any time an officer becomes aware of information relating to any type of hazard or activity that could adversely affect officers or citizens of the community, the officer shall communicate the nature of the hazard(s) on one of the following types of forms:
 - 1. **Bulletin** - This form may be used to disseminate various types of information. A variety of hazardous conditions can be brought to the attention of police department personnel as well as officers in other agencies throughout the state as well as the country.
 - 2. **Request for Extra Patrol** - This report advises of a hazardous condition or potential criminal problem for a given area in the city. The extra patrol is usually of short duration (a week or less) and names the location for the extra patrol, the nature of any problem expected, the person(s) involved, the suspect (if applicable), and which dispatcher or officer received the information.
 - 3. **Hazard Flags** - These messages advise of ongoing or long-term hazardous conditions at a given location. The information includes: location of the hazard, nature of the hazard and any persons involved. Officers at locations with hazard flags should take extra caution.
 - (a) Dispatchers will notify officers of any hazard flags on the calls for service locations they are assigned.
- (d) During the course of normal operations, officers may identify potential hazards to the safety of the citizens and which impact public safety response. Hazards may include weather (heavy rain, icy roads, snow, etc.), flooding, utility lines down, road hazards, etc.
- (e) The officer will immediately request the dispatcher to notify the appropriate agency/ department of the problem and request a response.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Administrative Communications

- (f) The officer will determine if it is necessary to implement traffic control measures (flares, detours, barricade requests, etc.), monitor the situation and notify the Public Works department if necessary.

203.5 ADMINISTRATIVE REPORTS

Administrative reporting allows the police department to isolate and identify problems and trends, and develop a pro-active approach to solving issues and/or problems internally and within the community.

- (a) Sergeants/Lieutenants shall complete daily shift logs at the end of each patrol shift. Logs will be completed using the electronic mail system and at a minimum shall include a brief description of major or noteworthy events and shift statistics.
 - 1. The log will be disseminated to the Chief of Police, Command Staff, Department Personnel, and others within the city as directed via the Group Police Log.
- (b) The Office of the Chief of Police, Division Commanders, and Sergeants may direct other reports to be completed concerning specific incidents, situations, presentations, research, or other items as needed for other purposes.

General Order

204.1 PURPOSE AND SCOPE

Departmental Orders establish an interdepartmental communication that may be used by the Chief of Police or his/her designee or a Division Commanders to give specific directions to departmental employees.

204.1.1 DEPARTMENTAL ORDER PROTOCOL

Any Departmental Orders issued after publication of the manual shall be numbered consecutively starting with the numeric numbering of the order followed by the last three digits of the year. For example, 001-08 signifies the first General Order for the year 2008.

Types of Departmental Orders are:

(a) Operational Orders:

1. Operational Orders are directives which are issued by the Chief of Police or his/her designee or a Division Commander intended to provide specific instructions for departmental personnel.
2. These orders are not policies; as they may add additional requirements or time constraints to existing policies that in general need not be dictated formally as policy.

(b) Special Orders:

1. Special Orders are directives which are issued by the Chief of Police or his/her designee or a Division Commander intended to provide specific instructions for special situations, events, training activities or official travel of departmental personnel.
2. These orders cover temporary situations and are self-canceling once the situation or event ceases to exist.

(c) Personnel Orders:

1. Personnel Orders are announcements of new employees, transfers of personnel to new assignments, promotions, separations, personal and group commendations, and other changes the status or assignment of personnel.
2. At the direction of the Police Chief or by the Deputy Chief of Police, personnel orders are prepared and issued by the applicable Division Commander.

204.2 ACCEPTANCE OF GENERAL ORDERS

All employees are required to read and obtain any necessary clarification of all General Orders. All employees are required to acknowledge in writing the receipt and review of any new General Order. Signed acknowledgement forms and/or e-mail receipts showing an employee's acknowledgement will be maintained by the Training Coordinator.

Retiree Concealed Firearms

205.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the issuance, denial, suspension or revocation of South Salt Lake Police Department identification cards under the Law Enforcement Officers' Safety Act (LEOSA) and Utah law (18 USC § 926C; Utah Code 53-5-704).

205.2 QUALIFIED RETIREES/FORMER OFFICERS

Participants must meet the following requirements:

- (a) Retired in good standing from service with a government agency as a law enforcement officer for an aggregate of 15 years or more for reasons other than mental instability, or retired from such an agency due to a service-connected disability after completing any applicable probationary period of such service
- (b) Was authorized by law to engage in or supervise the prevention, detection, investigation, prosecution or the incarceration of any person for any violation of law
- (c) had statutory powers of arrest
- (d) has a non-forfeitable right to benefits under the retirement plan of the agency for which (s)he was employed
- (e) meets, at his/her own expense, the same standards for qualification with a firearms as an active officer within the state in which he resides
- (f) is not under the influence of alcohol or another intoxicating or hallucinatory drug or substance
- (g) is not prohibited by federal law from possessing a firearm

205.3 MAINTAINING A CWL ENDORSEMENT

Only retired SSLPD officers in good standing are allowed to take part in the Retired Office Concealed Weapon Endorsement Program. Program requirements:

- (a) Applicants must submit a current criminal background clearance that can be obtained from the Division of Criminal Identification for \$10. Questions can be directed to BCI, (801) 965-4576.
- (b) Applicants must contact the SSLPD Training Unit (412-3600) for information on scheduled qualifications.
- (c) Applicants must read, understand and sign for receipt of an information bulletin detailing the provisions and limitations of 18 USCS 926 C.
- (d) Only Department instructors directed by SSLPD are eligible to administer the process and those instructors will have full authority to render a final decision on the applicant's skills and/or qualification.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Retiree Concealed Firearms

- (e) Applicants must utilize a weapon (handgun only) that is acceptable as outlined by current SSLPD Policy & Procedure.
- (f) The applicant is responsible for providing ammunition and any additional/alternate protective equipment desired.
- (g) Applicants must demonstrate marksmanship proficiency and safe handling skills during the course of fire that includes a variety of standing/kneeling/prone positions, strong and off-hand grips, at ranges from 3-25 yards.
- (h) A total of three (3) opportunities to qualify with a minimum of 80% will be allowed in a six-month period commencing with the first attempt.
- (i) Marksmanship and/or safe weapons handling training will not be provided.
- (j) All scores will be recorded and maintained in a file retained by the SSLPD Training Unit.
- (k) Photo identification cards will be issued only upon successful completion of the background and qualification process.
- (l) SSLPD retains the right to revoke or deny participation in the program to any participant that fails to meet minimum qualifications to include: unsafe practices, poor marksmanship and/or issues related to conduct.
- (m) SSLPD retains the right to amend, update and/or modify the program criteria based on the needs of the agency and/or to reflect changes in the law.
- (n) SSLPD reminds applicants that participation is entirely voluntary and that endorsements are conditional.
- (o) The City of South Salt Lake neither endorses nor indemnifies the actions of the program participants. The law does not extend a participant's authority to enforce the law in states where it is not already authorized, it simply gives participants greater freedom to be armed. The law (USCS 926 C) does not supersede or limit the laws of any State that:
 - 1. Permit private persons or entities to prohibit or restrict the possession of concealed firearms on their property.
 - 2. Prohibit or restrict the possession of firearms on any State or local government property, installation, building, base or park.
- (p) Furthermore, it is recommended that endorsement applicants secure legal advice and guidance before traveling to other states with concealed weapons
- (q) The applicant will indemnify and hold harmless SSLPD noting that participation in this program is voluntary and at their own risk.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Retiree Concealed Firearms

205.4 CARRYING FIREARMS OUT OF STATE

Subject to 18 USC § 926 B, 18 USC § 926 C and the Firearms and Qualification Policy, qualified retired officers of the Department may be authorized to carry a concealed weapon in other states.

205.5 DENIAL OR REVOCATION OF CWL ENDORSEMENT

The South Salt Lake City Police Department (SSLPD):

- (a) Retains the right to revoke or deny participation in the program to any participant that fails to meet minimum qualifications to include: unsafe practices, poor marksmanship and issues related to conduct. In addition, it is the prerogative of SSLPD to amend, update and/or modify the program criteria based on the needs of the agency and/or to reflect changes in the law.
- (b) Reminds applicants that participation is entirely voluntary and conditional.
- (c) The City of South Salt Lake neither endorses nor indemnifies the actions of the program participants. The law does not extend a participant's authority to enforce the law in states where it is not already authorized; it simply gives participants greater freedom to be armed. The law (USCS 926 C) does not supersede or limit the laws of any State that:
 - 1. permit private persons or entities to prohibit or restrict the possession of concealed firearms on their property or;
 - 2. Prohibit or restrict the possession of firearms on any State or local government property, installation, building, base or park.
- (d) Advises you to secure legal advice and guidance before traveling to other states with concealed weapons.
- (e) The applicant will indemnify and hold harmless SSLPD noting that participation in this program is at their own risk.
- (f) The law does not give officers the right to carry:
 - 1. any machine gun (as defined in section 5845 of the National Firearms Act);
 - 2. any firearm silencer (as defined in section 921 of Title 18); or
 - 3. any destructive device (as defined in section 921 of Title 18).

Chapter 3 - General Operations

Standards of Conduct

300.1 PURPOSE AND SCOPE

This policy establishes standards of conduct that are consistent with the values and mission of the South Salt Lake Police Department and are expected of all department members. The standards contained in this policy are not intended to be an exhaustive list of requirements and prohibitions but they do identify many of the important matters concerning conduct. In addition to the provisions of this policy, members are subject to all other provisions contained in this manual as well as any additional guidance on conduct that may be disseminated by this department or the member's supervisors.

300.2 POLICY

The continued employment or appointment of every member of the South Salt Lake Police Department shall be based on conduct that reasonably conforms to the guidelines set forth herein. Failure to meet the guidelines set forth in this policy, whether on- or off-duty, may be cause for disciplinary action.

300.2.1 POLICY

- (a) Discipline is a tool used for the channeling of individual effort into behavior and performance consistent with department objectives and accepted modes of conduct.
 - 1. It may include such activities as counseling, encouragement, reward, training, or the imposition of punishment.
 - 2. The use of punishment as a disciplinary measure is normally invoked only when other forms of discipline have not succeeded or when the gravity of the violation dictates its use for the good of the department.
- (b) Should an employee's performance, work habits, overall attitude, or conduct become unsatisfactory, based on violations of city or department policies, rules, or regulations, corrective or other disciplinary action should be considered. Such measures include, but are not limited to, the following:
 - 1. Training
 - (a) The employee's supervisor with or without the assistance of the training coordinator may arrange for the employee to receive initial or additional training to improve on his/ her performance, in the area where needed.
 - (b) This action will be documented and retained by the employee's supervisor and/ or may be placed in the employee's file.
 - (c) Training provides a positive method for altering unacceptable employee behavior by providing insight or review into the correct methods of a police operation and conduct.
 - (d) Training should not be administered as a punishment. Instead, it used and viewed as a positive learning experience for the employee, designed to correct a deficiency rather than to punish unacceptable performance.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Standards of Conduct

2. Counseling

- (a) A discussion of the employee's performance designed to provide constructive feedback without further discipline.
- (b) This action will be documented and retained by the supervisor.
- (c) Counseling also provides a positive method for seeking change in employee behavior. When a supervisor assumes the role of counselor the supervisor should consider the following elements.
- (d) The supervisor should attempt to determine whether the type of counseling needed is within the realm of his/her expertise.
- (e) Facts relevant to the employee's work history, prior disciplinary actions and present levels of performance should be reviewed prior to the counseling session.
- (f) Counseling should be in private and enough time should be allotted to ensure uninterrupted attention to the employee and the issues to be discussed.
- (g) The goal of any counseling session should be to make the employee aware of the reason for the counseling and to reach an agreement on what will take place to correct performance deficiencies.
- (h) All employees counseling sessions should be documented by the supervisor and retained in the supervisor's file.

3. Verbal warning

- (a) Whenever grounds for disciplinary action exist, and the Department Head or designee determines that more severe action is not immediately necessary, the deficiency demonstrated should be verbally communicated to the employee.
 - (b) A memorandum of the date and conduct of the verbal warning shall be written by the department head or designee.
 - (c) This memorandum shall be placed in a separate Verbal Warning folder in the Human Resource Department and is not part of the employee's personnel file.
- (c) When positive methods of discipline do not succeed, or when they are inappropriate to the violation being addressed, negative discipline is applied. When negative discipline is applied, the department will adhere to the City of South Salt Lake Policy Procedure Manual Section VI, Titled "Disciplinary Action."

300.3 CAUSES FOR DISCIPLINE

The following are illustrative of causes for disciplinary action. This list is not intended to cover every possible type of misconduct and does not preclude the recommendation of disciplinary action for violation of other rules, standards, ethics and specific action or inaction that is detrimental to efficient department service.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Standards of Conduct

300.3.1 LAWS, RULES AND ORDERS

- (a) Violation of, or ordering or instructing a subordinate to violate any policy, procedure, rule, order, directive, requirement or failure to follow instructions contained in department or City manuals.
- (b) Disobedience of any legal directive or order issued by any department member of a higher rank.
- (c) Violation of federal, state, local or administrative laws, rules or regulations.

300.3.2 ETHICS

- (a) Using or disclosing one's status as a member of the South Salt Lake Police Department in any way that could reasonably be perceived as an attempt to gain influence or authority for nondepartment business or activity.
- (b) The wrongful or unlawful exercise of authority on the part of any member for malicious purpose, personal gain, willful deceit, or any other improper purpose.
- (c) The receipt or acceptance of a reward, fee, or gift from any person for service incident to the performance of the member's duties (lawful subpoena fees and authorized work permits excepted).
- (d) Acceptance of fees, gifts, or money contrary to the rules of this department and/or laws of the state.
- (e) Offer or acceptance of a bribe or gratuity.
- (f) Misappropriation or misuse of public funds, property, personnel, or services.
- (g) The unauthorized personal use of public money or public property in violation of Utah Code § 76-8-402.
- (h) Any other failure to abide by the standards of ethical conduct.

300.3.3 DISCRIMINATION, OPPRESSION, OR FAVORITISM

Unless required by law or policy, discriminating against, oppressing, or providing favoritism to any person because of actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, age, disability, economic status, cultural group, veteran status, marital status, and any other classification or status protected by law, or intentionally denying or impeding another in the exercise or enjoyment of any right, privilege, power, or immunity, knowing the conduct is unlawful.

300.3.4 RELATIONSHIPS

- (a) Unwelcome solicitation of a personal or sexual relationship while on duty or through the use of one's official capacity.
- (b) Engaging in on duty sexual activity including, but not limited to, sexual intercourse, excessive displays of public affection or other sexual contact.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Standards of Conduct

- (c) Establishing or maintaining an inappropriate personal or financial relationship, as a result of an investigation, with a known victim, witness, suspect or defendant while a case is being investigated or prosecuted, or as a direct result of any official contact.
- (d) Associating with or joining a criminal gang, organized crime and/or criminal syndicate when the member knows or reasonably should know of the criminal nature of the organization. This includes any organization involved in a definable criminal activity or enterprise, except as specifically directed and authorized by this department.
- (e) Associating on a personal, rather than official basis with persons who demonstrate recurring involvement in serious violations of state or federal laws after the member knows, or reasonably should know of such criminal activities, except as specifically directed and authorized by this department.

300.3.5 ATTENDANCE

- (a) Leaving the job to which the member is assigned during duty hours without reasonable excuse and proper permission and approval.
- (b) Unexcused or unauthorized absence or tardiness.
- (c) Excessive absenteeism or abuse of leave privileges.
- (d) Failure to report to work or to the place of assignment at the time specified and fully prepared to perform duties without reasonable excuse.

300.3.6 UNAUTHORIZED ACCESS, DISCLOSURE OR USE

- (a) Unauthorized and inappropriate intentional release of confidential or protected information, materials, data, forms or reports obtained as a result of the member's position with this department.
- (b) Disclosing to any unauthorized person any active investigation information.
- (c) The use of any information, photograph, video or other recording obtained or accessed as a result of employment or appointment to this department for personal or financial gain or without the express authorization of the Chief of Police or the authorized designee.
- (d) Loaning, selling, allowing unauthorized use, giving away or appropriating any South Salt Lake Police Department badge, uniform, identification card or department property for personal use, personal gain or any other improper or unauthorized use or purpose.
- (e) Using department resources in association with any portion of an independent civil action. These resources include, but are not limited to, personnel, vehicles, equipment and nonsubpoenaed records.

300.3.7 EFFICIENCY

- (a) Neglect of duty.
- (b) Unsatisfactory work performance including but not limited to failure, incompetence, inefficiency, or delay in performing and/or carrying out proper orders, work

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Standards of Conduct

assignments, or the instructions of supervisors without a reasonable and bona fide excuse.

- (c) Concealing, attempting to conceal, removing, or destroying defective or incompetent work.
- (d) Unauthorized sleeping during on-duty time or assignments.
- (e) Failure to notify the Department within 24 hours of any change in residence address or contact numbers.
- (f) Failure to notify the Department of Human Resources of changes in relevant personal information (e.g., information associated with benefits determination) in a timely fashion.

300.3.8 PERFORMANCE

- (a) Failure to disclose or misrepresenting material facts, or making any false or misleading statement on any application, examination form, or other official document, report or form, or during the course of any workrelated investigation.
- (b) The falsification of any work-related records, making misleading entries or statements with the intent to deceive or the willful and unauthorized removal, alteration, destruction and/or mutilation of any department record, public record, book, paper or document.
- (c) Failure to participate in, or giving false or misleading statements, or misrepresenting or omitting material information to a supervisor or other person in a position of authority, in connection with any investigation or in the reporting of any departmentrelated business.
- (d) Being untruthful or knowingly making false, misleading or malicious statements that are reasonably calculated to harm the reputation, authority or official standing of this department or its members.
- (e) Disparaging remarks or conduct concerning duly constituted authority to the extent that such conduct disrupts the efficiency of this department or subverts the good order, efficiency and discipline of this department or that would tend to discredit any of its members.
- (f) Unlawful gambling or unlawful betting at any time or any place. Legal gambling or betting under any of the following conditions:
 - 1. While on department premises.
 - 2. At any work site, while on duty or while in uniform, or while using any department equipment or system.
 - 3. Gambling activity undertaken as part of an officer's official duties and with the express knowledge and permission of a direct supervisor is exempt from this prohibition.
- (g) Improper political activity including:
 - 1. Unauthorized attendance while on duty at official legislative or political sessions.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Standards of Conduct

- 2. Solicitations, speeches or distribution of campaign literature for or against any political candidate or position while on duty or, on department property or while in any way representing him/herself as a member of this department, except as expressly authorized by City policy, the collective bargaining agreement, or the Chief of Police.
- (h) Engaging in political activities during assigned working hours except as expressly authorized by City policy, the collective bargaining agreement, or the Chief of Police.
- (i) Any act on or off duty that brings discredit to this department.

300.3.9 CONDUCT

- (a) Failure of any member to promptly and fully report activities on his/her part or the part of any other member where such activities resulted in contact with any other law enforcement agency or that may result in criminal prosecution or discipline under this policy.
- (b) Unreasonable and unwarranted force to a person encountered or a person under arrest.
- (c) Exceeding lawful peace officer powers by unreasonable, unlawful or excessive conduct.
- (d) Unauthorized or unlawful fighting, threatening or attempting to inflict unlawful bodily harm on another.
- (e) Engaging in horseplay that reasonably could result in injury or property damage.
- (f) Discourteous, disrespectful or discriminatory treatment of any member of the public or any member of this department or the City.
- (g) Use of obscene, indecent, profane or derogatory language while on-duty or in uniform.
- (h) Criminal, dishonest, or disgraceful conduct, whether on- or off-duty, that adversely affects the member's relationship with this department.
- (i) Unauthorized possession of, loss of, or damage to department property or the property of others, or endangering it through carelessness or maliciousness.
- (j) Attempted or actual theft of department property; misappropriation or misuse of public funds, property, personnel or the services or property of others; unauthorized removal or possession of department property or the property of another person.
- (k) Activity that is incompatible with a member's conditions of employment or appointment as established by law or that violates a provision of any collective bargaining agreement to include fraud in securing the appointment or hire.
- (l) Initiating any civil action for recovery of any damages or injuries incurred in the course and scope of employment or appointment without first notifying the Chief of Police of such action.
- (m) Any other on- or off-duty conduct which any member knows or reasonably should know is unbecoming a member of this department, is contrary to good order, efficiency or morale, or tends to reflect unfavorably upon this department or its members.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Standards of Conduct

- (n) If the use of profanity occurs during the immediacy of an event as an apparent necessary escalation of force, then the officer will be encouraged not to use profanity. Profanity could be construed as unprofessional behavior. The officer will also be encouraged not to use profanity in the future. This is not subject to progressive discipline as long as there has not been an established pattern of the use of profanity.

300.3.10 SAFETY

- (a) Failure to observe or violating department safety standards or safe working practices.
- (b) Failure to maintain current licenses or certifications required for the assignment or position (e.g., driver's license, first aid).
- (c) Failure to maintain good physical condition sufficient to adequately and safely perform law enforcement duties.
- (d) Unsafe firearm or other dangerous weapon handling to include loading or unloading firearms in an unsafe manner, either on- or off-duty.
- (e) Carrying, while on the premises of the work place, any firearm or other lethal weapon that is not authorized by the member's appointing authority.
- (f) Unsafe or improper driving habits or actions in the course of employment or appointment.
- (g) Any personal action contributing to a preventable traffic collision.
- (h) Concealing or knowingly failing to report any on-the-job or work-related accident or injury as soon as practicable but within 24 hours.

300.3.11 INTOXICANTS

- (a) Reporting for work or being at work while intoxicated or when the member's ability to perform assigned duties is impaired due to the use of alcohol, medication or drugs, whether legal, prescribed or illegal.
- (b) Possession or use of alcohol at any work site or while on-duty, except as authorized in the performance of an official assignment. A member who is authorized to consume alcohol is not permitted to do so to such a degree that it may impair on-duty performance.
- (c) Unauthorized possession, use of, or attempting to bring a controlled substance, illegal drug or non-prescribed medication to any work site.

300.4 POST DISCIPLINE PROCEDURE

In situations resulting in the imposition of a suspension, punitive transfer, demotion, or termination of a non-probationary employee, the employee shall have the right to an evidentiary appeal of the Chief of Police's imposition of discipline pursuant to the City of South Salt Lake Personnel Policies and Procedures Manual.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Standards of Conduct

300.5 DIRECTIVES AND ORDERS

Members shall comply with lawful directives and orders from any [department/office] supervisor or person in a position of authority, absent a reasonable and bona fide justification. This includes any order relayed from a supervisor by a member of the same or lesser rank.

300.5.1 UNLAWFUL OR CONFLICTING ORDERS

Supervisors shall not knowingly issue orders or directives that, if carried out, would result in a violation of any law or department policy. Supervisors should not issue orders that conflict with any previous order without making reasonable clarification that the new order is intended to countermand the earlier order.

No member is required to obey any order that appears to be in direct conflict with any federal law, state law or local ordinance. Following a known unlawful order is not a defense and does not relieve the member from criminal or civil prosecution or administrative discipline. If the legality of an order is in doubt, the affected member shall ask the issuing supervisor to clarify the order or shall confer with a higher authority. The responsibility for refusal to obey rests with the member, who shall subsequently be required to justify the refusal.

Unless it would jeopardize the safety of any individual, members who are presented with a lawful order that is in conflict with a previous lawful order, department policy or other directive shall respectfully inform the issuing supervisor of the conflict. The issuing supervisor is responsible for either resolving the conflict or clarifying that the lawful order is intended to countermand the previous lawful order or directive, in which case the member is obliged to comply. Members who are compelled to follow a conflicting lawful order after having given the issuing supervisor the opportunity to correct the conflict, will not be held accountable for disobedience of the lawful order or directive that was initially issued.

The person countermanding the original order shall notify, in writing, the person issuing the original order, indicating the action taken and the reason.

300.5.2 SUPERVISOR RESPONSIBILITIES

Supervisors and managers are required to follow all policies and procedures and may be subject to discipline for:

- (a) Failure to be reasonably aware of the performance of their subordinates or to provide appropriate guidance and control.
- (b) Failure to promptly and fully report any known misconduct of a member to their immediate supervisor or to document such misconduct appropriately or as required by policy.
- (c) Directing a subordinate to violate a policy or directive, acquiescing to such a violation, or exhibiting indifference to such a violation.
- (d) Exercising unequal or disparate authority toward any member for malicious or other improper purpose.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Standards of Conduct

300.6 GENERAL STANDARDS

Members shall conduct themselves, whether on- or off-duty, in accordance with the United States and Utah constitutions and all applicable laws, ordinances, and rules enacted or established pursuant to legal authority.

Members shall familiarize themselves with policies and procedures and are responsible for compliance with each. Members should seek clarification and guidance from supervisors in the event of any perceived ambiguity or uncertainty.

Discipline may be initiated for any good cause. It is not mandatory that a specific policy or rule violation be cited to sustain discipline. This policy is not intended to cover every possible type of misconduct.

300.6.1 DUTY TO INTERVENE AND REPORT MISCONDUCT

An officer present and observing another officer engaging in police misconduct shall, when in a position to do so, intervene to stop the misconduct (Utah Code 53-6-210.5).

A member who witnesses police misconduct shall report the misconduct to a supervisor or [city/county] attorney, as applicable, as soon as practicable. Failure to report the misconduct is grounds for discipline by the [Department/Office] (Utah Code 53-6-210.5).

If the reported misconduct involves a law enforcement officer of another agency, the Chief of Police shall promptly notify and communicate the report to the chief executive of that law enforcement agency (Utah Code 53-6-210.5). Police misconduct means on-duty conduct by an officer that constitutes (Utah Code 53-6-210.5):

- (a) Force that is clearly beyond what is objectively reasonable under the totality of the circumstances or clearly does not amount to justified conduct (Utah Code 76-2-401 et seq.).
- (b) A search or seizure without a warrant where the totality of circumstances clearly indicates that any exception to the warrant requirement would not apply (see the Search and Seizure Policy).
- (c) Conduct that an objectively reasonable person would find to be biased or discriminatory against an individual or a group based on race, color, sex, pregnancy, age, religion, national origin, disability, sexual orientation, or gender identity.

The Chief of Police or the authorized designee should ensure that any additional applicable reporting requirements, anti-retaliatory practices, and disciplinary procedures set forth in Utah Code 53-6-210.5 are followed.

Bias-Based Policing

301.1 PURPOSE AND SCOPE

This policy provides guidance to department members that affirms the South Salt Lake Police Department's commitment to policing that is fair and objective (Utah Code 10-3-913; Utah Code 17-72-301; Utah Code 53-1-108).

Nothing in this policy prohibits the use of specified characteristics in law enforcement activities designed to strengthen the department's relationship with its diverse communities (e.g., cultural and ethnicity awareness training, youth programs, community group outreach and partnerships).

301.1.1 DEFINITIONS

Definitions related to this policy include:

Bias-based policing or improper profiling - An inappropriate reliance on actual or perceived characteristics such as race, ethnicity, national origin (including limited English proficiency), religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, disability, or affiliation with any non-criminal group (protected characteristics) as the basis for providing differing law enforcement service or enforcement (Utah Code 53-6-210.5). This includes explicit and implicit biases (i.e., conscious and unconscious beliefs or attitudes towards certain groups).

301.2 POLICY

The South Salt Lake Police Department is committed to providing law enforcement services to the community with due regard for the racial, cultural or other differences of those served. It is the policy of this department to provide law enforcement services and to enforce the law equally, fairly, objectively and without discrimination toward any individual or group.

301.3 BIAS-BASED POLICING PROHIBITED

Bias-based policing is strictly prohibited (Utah Code 53-6-210.5).

However, nothing in this policy is intended to prohibit an officer from considering protected characteristics in combination with credible, timely, and distinct information connecting a person or people of a specific characteristic to a specific unlawful incident, or to specific unlawful incidents, specific criminal patterns, or specific schemes.

301.4 MEMBER RESPONSIBILITIES

Every member of this department shall perform their duties in a fair and objective manner and is responsible for promptly reporting any suspected or known instances of bias-based policing to a supervisor. Members should, when reasonable to do so, intervene to prevent any bias-based actions by another member (Utah Code 53-6-210.5).

301.4.1 REASON FOR CONTACT

Officers contacting a person shall be prepared to articulate sufficient reason for the contact, independent of the protected characteristics of the individual.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Bias-Based Policing

To the extent that written documentation would otherwise be completed (e.g., arrest report, Field Interview (FI) card), the involved officer should include those facts giving rise to the contact, as applicable.

Except for required data-collection forms or methods, nothing in this policy shall require any officer to document a contact that would not otherwise require reporting.

301.5 SUPERVISOR RESPONSIBILITIES

Supervisors should monitor those individuals under their command for compliance with this policy and shall handle any alleged or observed violation of this policy in accordance with the Personnel Complaints Policy.

- (a) Supervisors should discuss any issues with the involved officer and the officer's supervisor in a timely manner.
 - 1. Supervisors should document these discussions in the prescribed manner.
- (b) Supervisors should periodically review Mobile Audio/Video (MAV) recordings, body-worn camera (BWC) media, Mobile Data Terminal (MDT) data, and any other available resource used to document contact between officers and the public to ensure compliance with this policy.
 - 1. Supervisors should document these periodic reviews.
 - 2. Recordings or data that capture a potential instance of bias-based policing should be appropriately retained for administrative investigation purposes.
- (c) Supervisors shall initiate investigations of any actual or alleged violations of this policy (Utah Code 53-6-211).
- (d) Supervisors should take prompt and reasonable steps to address any retaliatory action taken against any member of this [department/office] who discloses information concerning bias-based policing (Utah Code 53-6-210.5).

301.6 ADMINISTRATION

The Patrol Division Commander should review the efforts of the [Department/Office] to provide fair and objective policing and submit an annual report, including public concerns and complaints, to the Chief of Police. The report should also include a documented review of [department/office] activities with potential for bias. This may include traffic and field contacts, asset forfeiture efforts, citizen complaints, and any corrective measures taken. The annual report should not contain any identifying information about any specific complaint, member of the public, or officer. It should be reviewed by the Chief of Police to identify any changes in training or operations that should be made to improve service.

Supervisors should review the annual report and discuss the results with those they are assigned to supervise.

301.7 TRAINING

Training on fair and objective policing and review of this policy shall be conducted annually and include:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Bias-Based Policing

- (a) Explicit and implicit biases.
- (b) Avoiding improper profiling.

Officer Response to Calls

302.1 PURPOSE AND SCOPE

This policy provides for the safe and appropriate response to emergency and non-emergency situations whether dispatched or self-initiated.

302.2 RESPONSE TO CALLS

Officers dispatched "Code-3" shall consider the call an emergency response and proceed immediately. Officers responding Code-3 shall continuously operate emergency lighting equipment and shall sound the siren as reasonably necessary (Utah Code 41-6a-212).

Responding with emergency lights and siren does not relieve the officer operating an authorized emergency vehicle of the duty to act as a reasonably prudent emergency vehicle operator in like circumstances. The use of any other warning equipment without emergency lights and siren does not provide any privilege under the law.

Officers should only respond Code-3 when so dispatched or when circumstances reasonably indicate an emergency response is required. Officers not authorized to respond Code-3 shall observe all traffic laws and proceed without the use of emergency lights and siren.

302.2.1 POLICY

An "Authorized Emergency Vehicle" in this department is equipped with a siren and with authorized emergency warning lights. Vehicles not equipped with the preceding equipment, or vehicles with such equipment that is inoperative, will not be used as emergency vehicles.

(a) Routine Response

1. Officers will respond routinely or "Code 1" to all calls not designated as an emergency.
2. A "Code 1" response consists of operating the police vehicle by the most direct route to the call while adhering to all traffic regulations, speed limits, and rules of the road.
3. The use of emergency lights and siren during a "Code 1" response is not authorized.

(b) "Clearing an Intersection" for the purpose of this policy is defined as coming to a complete stop at a intersection regulated by a red light or stop sign, activating all emergency equipment, proceeding through the intersection at a safe speed, then discontinuing the use of emergency equipment.

1. Officers will not use this method when responding to unverified burglary alarms, in that they are inherently false, and the risk of this type of response is not justifiable.

(c) Emergency Vehicle Operation

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Officer Response to Calls

1. Officers may respond emergency mode or "Code 3" to all calls designated an emergency that require a faster police response than would occur if traffic laws were strictly obeyed.
2. Only sworn peace officers of the department will operate police vehicles during a "Code 3" response.
3. Whenever an officer initiates a "Code 3" response to an emergency call, he/she will advise the communications center of his/her location and his/her response mode.
4. Emergency warning lights and siren will be used at all times when operating "Code 3".
5. If the "Code 3" response is based on information initiated by the officer, the officer shall notify the communications center and receive acknowledgment.
6. The officer shall terminate his/her "Code 3" response at the earliest possible time.
7. The officer should get to the location of the event as quickly and safely as possible. An emergency response does not automatically authorize excessive speed of the patrol vehicle.
8. The operating speed of the vehicle shall be kept at a level which allows the officer to avoid hazards which may be reasonably anticipated, including coming to a stop at intersections until certain the intersection is clear or other drivers are yielding the right of way.
9. The responding officer must remain cognizant of the safety of himself/ herself and the general public.

(d) Emergency Calls

1. Officers may respond in emergency mode or "Code 3" while responding to the following types of incidents:
 - (a) Traffic accidents with injuries. (Primary unit only.)
 - (b) A life threatening medical emergency.
 - (c) Calls involving injured persons where the extent of injury is unknown.
 - (d) Any crime or hazard that immediately endangers human life.
 - (e) Calls assigned by the communications center that are designated as emergencies when dispatched.
 - (f) When directed by a supervisor.
 - (g) Another Officer needs assistance for personal safety.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Officer Response to Calls

- (h) Authorized vehicle pursuits are covered in the preceding section of this chapter.
- (e) Discontinuance of an Emergency Response
 - (a) Officers should not feel compelled to continue a "Code 3" response when conditions escalate to a degree that places the safety of the officer or others in jeopardy. Conditions, which must be evaluated continuously are:
 - (a) The capabilities of the officer to control the operation of the vehicle.
 - (b) Vehicle speed in relation to road conditions.
 - (c) The degree of emergency or threat to others.

302.3 REQUESTING EMERGENCY ASSISTANCE

Requests for emergency assistance should be limited to those situations where the involved personnel reasonably believe that there is an immediate threat to the safety of officers, or assistance is needed to prevent imminent serious harm to a citizen. In any event, where a situation has stabilized and emergency response is not required, the requesting officer shall immediately notify Dispatch.

If circumstances permit, the requesting officer should give the following information:

- The vehicle number
- The location
- The reason for the request and type of emergency
- The number of units required

302.3.1 NUMBER OF UNITS ASSIGNED

Normally, only one vehicle should respond to an emergency call Code-3 unless the Watch Commander or the field supervisor authorizes additional vehicles.

302.4 INITIATING CODE 3 RESPONSE

If an officer believes a Code-3 response to any call is appropriate, the officer shall immediately notify Dispatch. Generally, only one vehicle should respond Code-3 to any situation. Should another officer believe a Code-3 response is appropriate, Dispatch shall be notified and the Watch Commander or field supervisor will make a determination as to whether one or more officers driving Code-3 is appropriate.

302.5 RESPONSIBILITIES OF RESPONDING OFFICERS

Officers shall exercise sound judgment and care with due regard for life and property when responding to an emergency call. Officers shall reduce speed at all street intersections to such a degree that they shall have complete control of the vehicle.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Officer Response to Calls

The decision to continue a Code-3 response is at the discretion of the officer. If, in the officer's judgment, the roadway conditions or traffic congestion does not permit such a response without unreasonable risk, the officer may elect to respond to the call without the use of emergency lights and siren at the legal speed limit. In such an event, the officer should immediately notify Dispatch. An officer shall also discontinue the Code-3 response when directed by a supervisor.

Upon receiving authorization or determining a Code-3 response is appropriate, an officer shall immediately give the location from which he/she is responding.

302.6 SUPERVISORY RESPONSIBILITIES

Upon being notified that a Code-3 response has been initiated, the Watch Commander or the field supervisor shall verify the following:

- (a) The proper response has been initiated.
- (b) No more than those units reasonably necessary under the circumstances are involved in the response.
- (c) Affected outside jurisdictions are being notified as practical.

The field supervisor shall monitor the response until it has been stabilized or terminated and assert control by directing units into or out of the response if necessary. If, in the supervisor's judgment, the circumstances require additional units to be assigned a Code-3 response, the supervisor may do so.

It is the supervisor's responsibility to terminate a Code-3 response that, in his/her judgment is inappropriate due to the circumstances.

When making the decision to authorize a Code-3 response, the Watch Commander or the field supervisor should consider the following:

- The type of call
- The necessity of a timely response
- Traffic and roadway conditions
- The location of the responding units

302.7 FAILURE OF EMERGENCY EQUIPMENT

If the emergency equipment on the vehicle should fail to operate, the officer must terminate the Code-3 response and respond accordingly. In all cases, the officer shall notify the Watch Commander, field supervisor, or Dispatch of the equipment failure so that another vehicle may be assigned to the emergency response.

Use of Force

303.1 PURPOSE AND SCOPE

This policy provides guidance for determining reasonableness of use of force in particular circumstances. There is no way to identify every potential fact scenario that a member of this department will face which may lead to a need to use force. As such, this policy sets forth the relevant considerations that every member of this department is expected to use in making such decisions in a professional, impartial, and reasonable manner.

In addition to other applicable policies, the guidelines for the reasonable application of force contained in this policy shall apply to all potential use of force.

303.1.1 DEFINITIONS

Definitions related to this policy include (UAC R728-507-3):

Deadly force - Force reasonably anticipated and intended to create a substantial likelihood of causing death or very serious injury.

Feasible - Reasonably capable of being done or carried out under the circumstances to successfully achieve the arrest or lawful objective without increasing risk to the officer or another person.

Force - The application of physical techniques or tactics, chemical agents, or weapons to another person. It is not a use of force when a person allows him/herself to be searched, escorted, handcuffed, or restrained.

Imminent - Ready to take place; impending. Note that imminent does not mean immediate or instantaneous.

Totality of the circumstances - All facts and circumstances known to the officer at the time, taken as a whole, including the conduct of the officer and the subject leading up to the use of force.

303.2 POLICY

The use of force by law enforcement personnel is a matter of critical concern, both to the public and to the law enforcement community. Officers are involved on a daily basis in numerous and varied interactions and, when warranted, may use reasonable force in carrying out their duties.

Officers must have an understanding of, and true appreciation for, their authority and limitations. This is especially true with respect to overcoming resistance while engaged in the performance of law enforcement duties.

The [Department/Office] recognizes and respects the value of all human life and dignity without prejudice to anyone. Vesting officers with the authority to use reasonable force and to protect the public welfare requires monitoring, evaluation, and a careful balancing of all interests (UAC R728-507-5).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Use of Force

303.2.1 DUTY TO INTERVENE AND REPORT

Any officer present and observing another law enforcement officer or a member using force that is clearly beyond that which is objectively reasonable under the circumstances shall, when in a position to do so, intervene to prevent the use of unreasonable force (UAC R728-507-10).

Any officer who observes another law enforcement officer or a member use force that is potentially beyond that which is objectively reasonable under the circumstances shall report these observations to a supervisor as soon as feasible (UAC R728-507-10).

303.2.2 PERSPECTIVE

When observing or reporting force used by a law enforcement officer, each officer should take into account the totality of the circumstances and the possibility that other law enforcement officers may have additional information regarding the threat posed by the subject (UAC R728-507-10).

303.3 USE OF FORCE

Officers shall use only that amount of force that reasonably appears necessary given the facts and circumstances perceived by the officer at the time of the event to accomplish a legitimate law enforcement purpose (UAC R728-507-5).

The reasonableness of force will be judged from the perspective of a reasonable officer on the scene at the time of the incident. Any evaluation of reasonableness must allow for the fact that officers are often forced to make split-second decisions about the amount of force that reasonably appears necessary in a particular situation, with limited information and in circumstances that are tense, uncertain, and rapidly evolving.

Given that no policy can realistically predict every possible situation an officer might encounter, officers are entrusted to use well-reasoned discretion in determining the appropriate use of force in each incident (UAC R728-507-5).

It is also recognized that circumstances may arise in which officers reasonably believe that it would be impractical or ineffective to use any of the tools, weapons, or methods provided by this department. Officers may find it more effective or reasonable to improvise their response to rapidly unfolding conditions that they are confronting. In such circumstances, the use of any improvised device or method must nonetheless be reasonable and utilized only to the degree that reasonably appears necessary to accomplish a legitimate law enforcement purpose (UAC R728-507-5).

While the ultimate objective of every law enforcement encounter is to avoid or minimize injury, nothing in this policy requires an officer to retreat or be exposed to possible physical injury before applying reasonable force (UAC R728-507-5).

303.3.1 USE OF FORCE TO EFFECT AN ARREST

An officer may use reasonable force to effect arrest, to prevent escape, or to overcome resistance. An officer who makes or attempts to make an arrest need not retreat or desist from the officer's efforts by reason of resistance or threatened resistance of the person being arrested; nor shall such officer be deemed the aggressor or lose the officer's right to self-defense by the use of

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Use of Force

reasonable force to effect the arrest or to prevent escape or to overcome resistance (Utah Code 77-7-7; UAC R728-507-5).

303.3.2 FACTORS USED TO DETERMINE THE REASONABLENESS OF FORCE

When determining whether to apply force and evaluating whether an officer has used reasonable force, a number of factors should be taken into consideration, as time and circumstances permit. These factors include but are not limited to (UAC R728-507-5; UAC R728-507-7):

- (a) Immediacy and severity of the threat to officers or others.
- (b) The conduct of the individual being confronted, as reasonably perceived by the officer at the time.
- (c) Officer/subject factors (e.g., age, size, relative strength, skill level, injuries sustained, level of exhaustion or fatigue, the number of officers available vs. subjects).
- (d) The effects of suspected drug or alcohol use.
- (e) The individual's mental state or capacity.
- (f) The individual's ability to understand and comply with officer commands.
- (g) Proximity of weapons or dangerous improvised devices.
- (h) The degree to which the individual has been effectively restrained and the individual's ability to resist despite being restrained.
- (i) The availability of other reasonable and feasible options and their possible effectiveness.
- (j) Seriousness of the suspected offense or reason for contact with the individual.
- (k) Training and experience of the officer.
- (l) Potential for injury to officers, suspects, and others.
- (m) Whether the individual appears to be resisting, attempting to evade arrest by flight, or is attacking the officer.
- (n) The risk and reasonably foreseeable consequences of escape.
- (o) The apparent need for immediate control of the individual or a prompt resolution of the situation.
- (p) Whether the conduct of the individual being confronted no longer reasonably appears to pose an imminent threat to the officer or others.
- (q) Prior contacts with the individual or awareness of any propensity for violence.
- (r) Any other exigent circumstances.

303.3.3 PAIN COMPLIANCE TECHNIQUES

Pain compliance techniques may be effective in controlling a physically or actively resisting individual. Officers may only apply those pain compliance techniques for which they have successfully completed [department/office]-approved training (UAC R728-507-7). Officers utilizing any pain compliance technique should consider:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Use of Force

- (a) The degree to which the application of the technique may be controlled given the level of resistance.
- (b) Whether the individual can comply with the direction or orders of the officer.
- (c) Whether the individual has been given sufficient opportunity to comply.

The application of any pain compliance technique shall be discontinued once the officer determines that compliance has been achieved (UAC R728-507-7).

303.3.4 USE OF FORCE TO SEIZE EVIDENCE

In general, officers may use reasonable force to lawfully seize evidence and to prevent the destruction of evidence. However, officers are discouraged from using force solely to prevent a person from swallowing evidence or contraband. In the instance when force is used, officers shall not intentionally use any technique that restricts blood flow to the head, restricts respiration or which creates a reasonable likelihood that blood flow to the head or respiration would be restricted. Officers are encouraged to use techniques and methods taught by the South Salt Lake Police Department for this specific purpose.

303.3.5 ALTERNATIVE TACTICS - DE-ESCALATION

When circumstances reasonably permit, officers should use non-violent strategies and techniques to decrease the intensity of a situation, improve decision-making, improve communication, reduce the need for force, and increase voluntary compliance (e.g., summoning additional resources, formulating a plan, attempting verbal persuasion) (UAC R728-507-5).

303.3.6 DEFENSIVE TACTICS

Officers who have successfully completed [department/office]-approved training may apply defensive tactic techniques, including but not limited to focused strikes that involve the use of empty-hand techniques and contact control measures (UAC R728-507-8).

303.3.7 KNEE ON NECK RESTRAINT

An officer shall not restrain a person by the application of a knee applying pressure to the neck or throat of a person (Utah Code 53-13-115).

303.4 DEADLY FORCE APPLICATIONS

When reasonable, the officer shall, prior to the use of deadly force, make efforts to identify the officer as a peace officer and to warn that deadly force may be used, unless the officer has objectively reasonable grounds to believe the person is aware of those facts (UAC R728-507-6).

Use of deadly force is justified in the following circumstances involving an imminent threat or an imminent risk (Utah Code 76-2-404; UAC R728-507-6):

- (a) An officer may use deadly force to protect the officer or an individual other than the suspect from what the officer reasonably believes is an imminent threat of death or serious bodily injury.
- (b) An officer may use deadly force to stop a fleeing subject when the officer has probable cause to believe that the individual has committed, or intends to commit, a felony

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Use of Force

involving the infliction or threatened infliction of serious bodily injury or death, and the officer reasonably believes that there is an imminent risk of serious bodily injury or death to an individual other than the suspect if the suspect is not immediately apprehended. Under such circumstances, a verbal warning should precede the use of deadly force, where feasible.

However, an officer shall not use deadly force against a person whose actions are a threat solely to themselves or property unless the person poses an imminent danger of death or serious physical injury to the officer or others in close proximity.

Imminent does not mean immediate or instantaneous. An imminent danger may exist even if the suspect is not at that very moment pointing a weapon at someone. For example, an imminent danger may exist if an officer reasonably believes that the suspect has a weapon or is attempting to access one and intends to use it against the officer or an individual other than the suspect. An imminent danger may also exist if the suspect is capable of causing serious bodily injury or death without a weapon, and the officer believes the individual intends to do so.

Unless deadly force is justified, officers shall not apply pressure to a person's neck that is sufficient to make breathing difficult or impossible, including, but not limited to, any pressure to the throat or windpipe that may prevent or hinder breathing or reduced intake of air (choke holds).

303.4.1 MOVING VEHICLES

Shots fired at or from a moving vehicle are rarely effective and involve considerations and risks in addition to the justification for the use of deadly force (UAC R728-507-6).

When feasible, officers should take reasonable steps to move out of the path of an approaching vehicle instead of discharging their firearm at the vehicle or any of its occupants (UAC R728-507-6).

An officer shall only discharge a firearm at a moving vehicle or its occupants when the officer reasonably believes there are no other reasonable means available to avert the imminent threat of the vehicle, or if deadly force other than the vehicle is directed at the officer or others (UAC R728-507-6).

Officers should not shoot at any part of a vehicle in an attempt to disable the vehicle (UAC R728-507-6).

An officer shall not discharge a firearm from a moving vehicle, except in exigent circumstances. In these situations, an officer must have articulable reason for this use of deadly force.

303.5 REPORTING THE USE OF FORCE

Any use of force by a member of this department shall be immediately reported to the on-duty supervisor and documented promptly, completely, and accurately in an appropriate report according to the nature of the incident. The Versaterm Use of Force Detail page shall be completed with each Use of Force incident. The officer who used force must report such use of force to the on-duty sergeant. Additionally, any officer that is aware or becomes aware of a use of force incident that may not have been reported to a supervisor is required to report the use of force to a

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Use of Force

supervisor. In reporting a use of force, the officer using force should articulate the factors perceived and why he/she believed the use of force was reasonable under the circumstances. To collect data for purposes of training, resource allocation, analysis, and related purposes, the Department may require the completion of additional report forms, as specified in department policy, procedure, or law (UAC R7 28-507-7) See the Report Preparation Policy for additional circumstances that may require documentation.

303.5.1 USE OF FORCE SUPERVISORY NOTIFICATION

Supervisory notification shall be made as soon as practicable following the application of force in any of the following circumstances:

- (a) When any Arrest Control Tactic (ACT) is used (beyond compliant handcuffing) to place a person into custody or to detain them for investigation.
- (b) When an officer discharges a firearm, points or displays (removed from holster) a firearm at any individual.
- (c) When an officer discharges, points or displays (low ready) a Taser at an individual.
- (d) When an officer discharges a pepper spray canister (Capsaicin) at or towards an individual.
- (e) When an officer intentionally damages the property of another to affect an arrest. (Damage to property under any other circumstance, shall be documented appropriately in a the Officer's written report.)
- (f) When a Police Service Dog (PSD) is deployed for the purpose of apprehending a suspect(s) or when verbal warnings are given that a PSD will be deployed for the purpose or intent of apprehension.
- (g) Any other application of force that results in injury of a person or animal.
- (h) Medical attention shall be immediately requested to respond to assist treatment needs.
- (i) The application of force caused a visible injury
- (j) The application of force would lead a reasonable officer to conclude that the individual may have experienced more than momentary discomfort
- (k) The individual subjected to the force complained of injury or continuing pain.
- (l) The individual indicates intent to pursue litigation.
- (m) Any application of a restraint device other than handcuffs, shackles, or belly chains.
- (n) The individual subjected to the force was rendered unconscious.
- (o) An individual was struck or kicked.
- (p) An individual alleges unreasonable force was used or that any application of force of the above has occurred.

303.5.2 ON-DUTY SUPERVISORY USE OF FORCE REVIEW RESPONSIBILITIES

- (a) If practicable, the on-duty supervisor shall respond to the scene where the use of force was used.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Use of Force

- (b) The on-duty supervisor shall gather all witness information and statements from any person who witnessed the incident. In the event a witness refuses to provide a statement the supervisor shall document their attempts to get a statement in the Use of Force Review.
- (c) The on-duty supervisor shall obtain the basic facts from the involved officer(s). Absent an allegation of misconduct or excessive force, this will be considered a routine contact in the normal course of duties.
- (d) The on-duty supervisor shall ensure any officer using force completes a detailed written report of the incident, including a description of the factors present in determining that the officer's use of force was reasonable. Documentation of the officer's use of force shall be set forth in a report drafted prior to the end of their shift, if practicable. If an officer is unable to complete a report prior to the end of their shift due to circumstances outside of the officer's control, the on-duty supervisor shall ensure the report is drafted as soon as possible thereafter and document the reasons for the delay.
 - 1. Notwithstanding the foregoing, an officer who is the subject of an OICI investigation (Policy- Officer Involved Shootings and Death) shall not be compelled to complete a detailed report of the incident.
- (e) Any officers involved or who witnesses a use of force incident shall provide a detailed report of their observations in a supplemental report.
- (f)
- (g) The on-duty supervisor shall notify the appropriate Lieutenant of any use of force review.
- (h) The on-duty supervisor shall ensure that any known injured parties are examined and treated by medical personnel.
- (i) Once any initial medical assessment has been completed or first aid has been rendered, the on-duty supervisor shall obtain photographs of any area involving visible injury or complaint of pain, as well as overall photographs of uninjured areas.
- (j) The on-duty supervisor shall review and approve all related reports
- (k)

303.5.3 SUPERVISOR USE OF FORCE REVIEW INITIATION RESPONSIBILITIES

In an effort to conduct a thorough review, a supervisor will conduct the initial review of all use of force incidents. The use of force review shall be initiated upon notification of the incident and as soon as possible following the incident. The initial review will be conducted by rank order at least one level higher than any officer directly involved in the use of force incident. The supervisor assigned to conduct the use of force review will adhere to the following criteria.

- (a) An on-duty sergeant will conduct the initial review of use of force incidents.
- (b) In the event, a sergeant is directly involved in the use of force incident the initial review will be conducted by a lieutenant.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Use of Force

- (c) In the event, a lieutenant is directly involved in the use of force incident the initial review will be conducted by a deputy chief.
- (d) In the event the Deputy Chief and/or Chief of Police are directly involved in the use of force incident the review will be conducted by the Chief of Police or designee at the discretion of the Chief of Police.
- (e) The supervisor assigned to conduct the initial review shall review all videos (body and in-car camera footage) associated with incident and properly classify and retain.
- (f) The supervisor assigned to conduct the initial review shall evaluate the circumstances surrounding the incident and make findings as to whether the officer(s) actions are compliant with department policy.
- (g) If there is a question of policy non-compliance or if for any reason further investigation may be appropriate, the supervisor assigned to conduct the review shall initiate an administrative investigation.

All Use of Force reviews require two levels of review. The second level supervisor review shall be conducted by a rank order at least one level higher than any officer directly involved in the use of force incident.

- (a) The second level supervisor shall:
 - 1. Review the use of force documentation to determine whether there are policy, training, weapons/equipment, or discipline issues that should be addressed.
 - 2. Forward all use of force reviews up the chain of command for review and tracking.
 - 3. For incidents involving the discharge of a firearm, immediately forward through the chain of command for review in accordance with Officer-Involved Shooting and Death Policy.
 - 4. Immediately notify the Chief's Office (Chief of Police or Deputy Chief) for any use of force in which there is evidence that the force used was unreasonable or there is evidence of a policy violation.
 - 5. In the event the Chief of Police and/or Deputy Chief are directly involved in the use of force, the second review will be conducted by the Chief of Police or designee at the discretion of the Chief of Police.

303.5.4 REPORTING THE THREAT OF FORCE

When an officer points a firearm at an individual, the officer shall report the incident in accordance with Utah Code 53-13-116 and UAC R728-507-12.

Reports shall be submitted within 48 hours of the incident and should include at a minimum (Utah Code 53-13-116; UAC R728-507-12):

- (a) A description of the incident.
- (b) The identification of the individuals involved in the incident.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Use of Force

303.6 MEDICAL CONSIDERATIONS

Once it is reasonably safe to do so, medical assistance shall be obtained for any person who exhibits signs of physical distress, has sustained visible injury, expresses a complaint of injury or continuing pain, or was rendered unconscious (UAC R728-507-7; UAC R728-507-11). Any individual exhibiting signs of physical distress after an encounter should be continuously monitored until the individual can be medically assessed. Individuals should not be placed on their stomachs for an extended period, as this could impair their ability to breathe.

Based upon the officer's initial assessment of the nature and extent of the individual's injuries, medical assistance may consist of examination by an emergency medical services provider or medical personnel at a hospital or jail. If any such individual refuses medical attention, such a refusal shall be fully documented in related reports and, whenever practicable, should be witnessed by another officer and/or medical personnel (UAC R728-507-11). If a recording is made of the contact or an interview with the individual, any refusal should be included in the recording, if possible.

The on-scene supervisor or, if the on-scene supervisor is not available, the primary handling officer shall ensure that any person providing medical care or receiving custody of a person following any use of force is informed that the person was subjected to force. This notification shall include a description of the force used and any other circumstances the officer reasonably believes would be potential safety or medical risks to the subject (e.g., prolonged struggle, extreme agitation, impaired respiration).

Individuals who exhibit extreme agitation, violent irrational behavior accompanied by profuse sweating, extraordinary strength beyond their physical characteristics, and imperviousness to pain, or who require a protracted physical encounter with multiple officers to be brought under control, may be at an increased risk of sudden death. Calls involving these persons should be considered medical emergencies. Officers who reasonably suspect a medical emergency should request medical assistance as soon as practicable and have medical personnel stage away (UAC R728-507-11).

See the Medical Aid and Response Policy for additional guidelines.

303.7 TRAINING

Officers shall receive annual training on this policy and demonstrate their knowledge and understanding.

Subject to available resources, officers should receive periodic training on guidelines regarding vulnerable populations, including but not limited to children, elderly, pregnant persons, and individuals with physical, mental, or intellectual disabilities.

303.7.1 TRAINING REQUIREMENTS

Required annual training shall include:

- (a) Legal updates.
- (b) De-escalation tactics, including alternatives to force.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Use of Force

- (c) The duty to intervene.
- (d) The duty to request and/or render medical aid.
- (e) Warning shots (see the Firearms Policy).
- (f) All other subjects covered in this policy (e.g., use of deadly force, chokeholds and carotid holds, discharge of a firearm at or from a moving vehicle, verbal warnings).

303.8 USE OF FORCE TRACKING SYSTEM

The [Department/Office] shall establish a system for tracking use of force incidents, and follow the Performance History Audits Policy for guidelines regarding monitoring and remediating use of force patterns for officers. South Salt Lake Police Department is utilizing a third party vendor (Guardian) to input, record, review, monitor, and identify the need for remediation of use of force.

Use of Force Review Boards

304.1 PURPOSE AND SCOPE

This policy establishes a process for the South Salt Lake Police Department to review the use of force by its employees.

This review process shall be in addition to any other review or investigation that may be conducted by any outside or multi-agency entity having jurisdiction over the investigation or evaluation of the use of force.

304.2 POLICY

The South Salt Lake Police Department will objectively evaluate the use of force by its members to ensure that their authority is used lawfully, appropriately and is consistent with training and policy.

304.3 REMOVAL FROM LINE DUTY ASSIGNMENT

Generally, whenever an employee's actions or use of force in an official capacity, or while using [department/office] equipment, results in death or serious injury to another, that employee will be placed in a temporary administrative assignment pending an administrative review. The Chief of Police may exercise discretion and choose not to place an employee in an administrative assignment.

However, any member who uses deadly force shall be removed from line duty assignment pending an administrative review.

304.4 REVIEW BOARD

The Use of Force Review Board will be convened when the use of force by a member per the City of South Salt Lake Civilian Review Board (CRB), in accordance with the City of South Salt Lake (SSL) Ordinance 2022-10.

.

Search and Seizure

305.1 PURPOSE AND SCOPE

Both the federal and state constitutions provide every individual with the right to be free from unreasonable searches and seizures. This policy provides general guidelines for South Salt Lake Police Department personnel to consider when dealing with search and seizure issues.

305.1.1 DEFINITIONS

- (a) **Exigent Circumstances** - Circumstances that require immediate action and/or remedy.
- (b) **First-Touch Pat-Down** - A police action in which a search of a suspect/arrestee is done by only touching the outside of the person's clothing and only making a quick contact to check for obvious weapons and/or contraband. Officers may not reach into the clothing unless an object distinctly feels like a weapon and/or contraband.
- (c) **Search** - A police action which infringes upon a persons reasonable expectation of privacy.
- (d) **Seizure of Property** - A significant interference by police, with an evidentiary interest in property.

305.2 POLICY

It is the policy of the South Salt Lake Police Department to respect the fundamental privacy rights of individuals. Members of this [department/office] will conduct searches in strict observance of the constitutional rights of persons being searched. All seizures by this [department/office] will comply with relevant federal and state law governing the seizure of persons and property.

The [Department/Office] will provide relevant and current training to officers as guidance for the application of current law, local community standards, and prosecutorial considerations regarding specific search and seizure situations, as appropriate.

305.2.1 POLICY

- (a) Warrant-less searches and seizures may be conducted only when exigent circumstances and/or probable cause exist.
 - 1. All items seized must be handled according to department policies and procedures.
- (b) Officers must consider the following when conducting a search and/or seizure without a warrant:
 - 1. Search by consent
 - (a) Whenever possible, officers will obtain the signature of the person being searched or the signature of a person who has proper authority to permit a search, on a department "Consent to Search" form.
 - (b) Officers will cease a search if the person(s) being searched upon request.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Search and Seizure

- (c) Officers will not intimidate or otherwise coerce any person into permitting a search.
 - (d) Officers should return any personal items belonging to the individual(s), such as driver's license, vehicle registration, etc., before asking for permission to search.
- 2. Stop and frisk
 - (a) Officers may do a pat-down search only if they feel that there is reason to believe that the person(s):
 - 1. Has committed or is in the act of committing a crime (UCA 77-7-15).
 - 2. Is in possession of a dangerous weapon and that the officers and/or other persons may be in danger (UCA 77-7-16).
 - 3. If a weapon is found during a pat-down search, the officers may retain the weapon until the completion of questioning, at which time it shall either be returned to the person or booked into evidence upon arrest (UCA 77-7-17).
 - 4. Officers may do only a "first-touch" pat-down search. If the officer determines that the person is not concealing a weapon, he/she may not continue with a second pat-down or prolonged touching of any certain area of the person, since this could then be considered a search and invalidate evidentiary value of any seized items.
- 3. Search of a vehicle
 - (a) If a vehicle is stopped for a traffic violation, the officer should complete the citation or warning process, including the return of the driver's license and/or vehicle registration, before conducting any legal search of a vehicle, unless the officer feels that there is a possibility of danger to himself/herself or any other person(s).
 - (b) An officer may "frisk" a vehicle if he/she has reasonable fears, based on specific and articulable facts, that his/her safety is threatened by the possible presence of a weapon in the vehicle. (Terry v. Ohio ruling, 392 U.S.1, 1968).
 - (c) The vehicle frisk is limited to the driver and passenger compartment area of the vehicle, which is within the driver's reach.
 - (d) Any contraband or other incriminating evidence found at this time may be seized.
 - (e) An officer may search a vehicle when the search is incident to arrest of occupant(s) of the vehicle. The officer may search only the areas of the vehicle, which are accessible to the person(s) being arrested.
 - (f) An officer may conduct a search of a vehicle if there is probable cause to believe that the vehicle contains fruits, instrumentalities or evidence of a crime or contraband (Carroll v. United States, 267 U.S. 132, 1925).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Search and Seizure

- (g) This search may include all parts of a vehicle.
- (h) This search may be conducted only when there is true probable cause enough to justify the issuance of a search warrant by a court.
- (i) If the officer has any doubts about the legality of a search, he/she should contact his/her shift supervisor for permission to detain the vehicle and its occupants until a search warrant can be obtained.
- (j) The time of detainment must not be longer than is "reasonably" necessary.

4. Inventory

- (a) Contents of a vehicle will be inventoried if the vehicle is seized or impounded.
 - (a) An inventory is not a search and must not be preformed in an investigatory manner.
- (b) The purpose of the vehicle inventory is:
 - (a) To protect the contents of the vehicle from loss.
 - (b) To protect the department against civil claims for loss.
 - (c) To protect the officers and public from hazardous substances or instrumentalities which may be contained in the vehicle.
- (c) The inventory will be written, and will be thorough to include all items of value located in the vehicle.
- (d) All evidence seized in the inventory will be placed in the evidence locker to ensure safekeeping.
- (e) The inventory will become part of the case file.
- (f) When custody of the vehicle changes from one person to another, the person taking custody of the vehicle will also assume custody of the contents by placing his or her signature on the inventory list.
- (g) The written inventory of vehicle's contents will include, but is not limited to:
 - (a) Items found in opened, closed, and locked containers, including in bags and boxes.
 - (b) Items found in any compartment of the vehicle.
 - (c) Items found in the trunk or under the hood of the vehicle.
 - (d) Items found under or between the seats of the vehicle.
- (h) Containers that would be damaged if forced open, such as locked briefcases and luggage, should only be opened in the presence of a supervising officer.
- (i) All inventories should be documented on a department vehicle inventory form, which should be attached to the report form.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Search and Seizure

5. An officer may conduct a complete search of the vehicle and its contents if he/she discovers contraband, weapons, and or evidence of a crime during the vehicle inventory.
 - (a) If reasonable, a search warrant should be obtained before conducting any search.
6. Officers may conduct searches and seizures based on other situations that are authorized by state and federal constitutional provisions.

305.3 SEARCHES

The U.S. Constitution generally provides that a valid warrant is required in order for a search to be valid. There are, however, several exceptions that permit a warrantless search.

Examples of law enforcement activities that are exceptions to the general warrant requirement include, but are not limited to, searches pursuant to the following:

- Valid consent
- Incident to lawful arrest
- Legitimate community caretaking interests
- Vehicle searches under certain circumstances
- Exigent circumstances

Certain other activities are recognized by federal and state courts and by certain statutes as legitimate law enforcement activities that also do not require a warrant. Such activities may include seizure and examination of abandoned property, and observations of activities and property located on open public areas.

Because case law regarding search and seizure is constantly changing and subject to interpretation by the courts, each member of this [department/office] is expected to act in each situation according to current training and their familiarity with clearly established rights as determined by case law.

Whenever practicable, officers are encouraged to contact a supervisor to resolve questions regarding search and seizure issues prior to electing a course of action.

305.3.1 PAROLE SEARCHES

Absent a search warrant or other legal authority an officer may search the residence of a person on parole only after obtaining approval from a parole officer. In other circumstances where an officer stops a parolee and conducts a search of the parolee's person, personal effects or vehicle, the officer shall notify a parole officer as soon as reasonably practicable after conducting the search (Utah Code 77-23-301(3)(a) and (b)).

Officers shall not request or conduct a parole search for the purpose of harassment (Utah Code 77-23-301(4)).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Search and Seizure

305.3.2 ELECTRONIC INFORMATION AND DATA

Officers shall follow warrant and notification requirements when (Utah Code 77-23c-101 et seq.; Utah Code 77-23f-101 et seq.):

- (a) Seeking reverse-location.
- (b) Seeking reverse-keyword information.
- (c) Seeking electronic data transmitted to a provider of a remote computing service or electronic communication service.

305.4 SEARCH PROTOCOL

Although conditions will vary and officer safety and other exigencies must be considered in every search situation, the following guidelines should be followed whenever circumstances permit:

- (a) Members of this [department/office] will strive to conduct searches with dignity and courtesy.
- (b) Officers should explain to the person being searched the reason for the search and how the search will be conducted.
- (c) Searches should be carried out with due regard and respect for private property interests and in a manner that minimizes damage. Property should be left in a condition as close as reasonably possible to its pre-search condition.
- (d) In order to minimize the need for forcible entry, an attempt should be made to obtain keys, combinations, or access codes when a search of locked property is anticipated.
- (e) When the person to be searched is of the opposite sex as the searching officer, a reasonable effort should be made to summon an officer of the same sex as the subject to conduct the search. When it is not practicable to summon an officer of the same sex as the subject, the following guidelines should be followed:
 - 1. Another officer or a supervisor should witness the search.
 - 2. The officer should not search areas of the body covered by tight-fitting clothing, sheer clothing, or clothing that could not reasonably conceal a weapon.

305.5 DOCUMENTATION

Officers are responsible to document any search and to ensure that any required reports are sufficient including, at minimum, documentation of the following:

- Reason for the search
- Any efforts used to minimize the intrusiveness of any search (e.g., asking for consent or keys)
- What force, if any, was used to execute the search
- Whether an announcement was made prior to or after entry into the premises
- What, if any, injuries or damage occurred
- All steps taken to secure property

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Search and Seizure

- The results of the search, including a description of any property or contraband seized
- If the person searched is the opposite sex, any efforts to summon an officer of the same sex as the person being searched and the identification of any witness officer

Supervisors shall review reports to ensure the reports are accurate, that actions are properly documented, and that current legal requirements and [department/office] policy have been met.

Strip Search and/or Body Cavity Search

306.1 PURPOSE AND SCOPE

Strip and body cavity searches are sometimes necessary for agency safety and security, or to seize evidence of criminal activity. These searches, however, are highly intrusive and shall be conducted within the limits of legal authority.

- (a) Strip and body cavity searches may be conducted only after obtaining a search warrant. Officers should consult a supervisor and the City Attorney before obtaining the search warrant.
- (b) An officer may use reasonable force to search the mouth of a person if the officer has probable cause to believe that the person has put property of evidentiary value into his/her mouth for the purpose of concealing or destroying the property.
- (c) The anus or vagina may be subject to a VISUAL search only in exigent circumstances. This visual search is to be conducted by an officer of the same sex or by someone of the same sex acting in the officer's aid and witnessed by a supervisor of the same sex.
- (d) Any search that requires a person to expose his/her genitals, anus, buttocks, or the female breast shall be conducted in a private setting, with due regard for human dignity, and must be witnessed by a supervisor of the same sex. The mouth may be searched without regard to privacy.
- (e) The search of the anus or vagina by touch, instrument, or other invasive measures, and the search of the stomach or intestines, shall require a search warrant and may be conducted only by a physician.
- (f) Anytime a strip or body cavity search is conducted a complete report of the incident and actions taken shall be submitted.
- (g) The submitted report shall be reviewed for accuracy and content by the supervisor who observed the search, if one was present.

Control Devices and Techniques

307.1 PURPOSE AND SCOPE

This policy provides guidelines for the use and maintenance of control devices that are described in this policy.

307.2 POLICY

In order to control subjects who are violent or who demonstrate the intent to be violent, the South Salt Lake Police Department authorizes officers to use control devices in accordance with the guidelines in this policy and the Use of Force Policy.

307.3 ISSUING, CARRYING AND USING CONTROL DEVICES

Control devices described in this policy may be carried and used by members of this department only if the device has been issued by the Department or approved by the Chief of Police or the authorized designee.

Only officers who have successfully completed department-approved training in the use of any control device are authorized to carry and use the device.

Control devices may be used when a decision has been made to control, restrain or arrest a subject who is violent or who demonstrates the intent to be violent, and the use of the device appears reasonable under the circumstances. When reasonable, a verbal warning and opportunity to comply should precede the use of these devices.

When using control devices, officers should carefully consider potential impact areas in order to minimize injuries and unintentional targets.

307.4 RESPONSIBILITIES

307.4.1 WATCH COMMANDER RESPONSIBILITIES

The Watch Commander may authorize the use of a control device by selected personnel or members of specialized units who have successfully completed the required training.

307.4.2 FIREARMS SUPERVISOR RESPONSIBILITIES

The Firearms Supervisor shall control the inventory and issuance of all control devices and shall ensure that all damaged, inoperative, outdated or expended control devices or munitions are properly disposed of, repaired or replaced.

Every control device will be periodically inspected by the Firearms Supervisor or the designated instructor for a particular control device. The inspection shall be documented.

307.4.3 USER RESPONSIBILITIES

All normal maintenance, charging or cleaning shall remain the responsibility of personnel using the various devices.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Control Devices and Techniques

Any damaged, inoperative, outdated or expended control devices or munitions, along with documentation explaining the cause of the damage, shall be returned to the Firearms Supervisor for disposition. Damage to City property forms shall also be prepared and forwarded through the chain of command, when appropriate, explaining the cause of damage.

307.5 BATON GUIDELINES

The need to immediately control a suspect must be weighed against the risk of causing serious injury. The head, neck, throat, spine, heart, kidneys and groin should not be intentionally targeted except when the officer reasonably believes the suspect poses an imminent threat of serious bodily injury or death to the officer or others.

When carrying a expandable baton, uniformed personnel shall carry the baton in its authorized holder on the equipment belt. Plainclothes and non-field personnel may carry the expandable baton as authorized and in accordance with the needs of their assignment or at the direction of their supervisor.

307.5.1 DEPARTMENT APPROVED EXPANDABLE BATONS

The expandable baton should be used when other means of non-lethal force is unreasonable or ineffective, and deadly force is not justified.

When feasible, a verbal warning will be given before using the expandable baton.

An officer shall never alter a expandable baton from factory specifications. This does not restrict the use of an aftermarket grip cap that has been approved by the Expandable Baton Force on Force Instructor.

The expandable baton is not to be used as a control technique to the throat/neck area.

The preferred target areas of the human body includes:

- Lower Legs.
- Arms and/or hands.
- Stomach/Chest area (center body mass)

Note: The expandable baton is not a mandatory piece of equipment and will be purchased by the officer. The expandable baton must be all black in color when fully extended; must be of high quality in manufacture and workmanship (i.e. ASP / Monadnock / Smartlock) and meet the approval of the Expandable Baton Force on Force Instructor.

307.6 TEAR GAS GUIDELINES

Tear gas may be used for crowd control, crowd dispersal or against barricaded suspects based on the circumstances. Only the Watch Commander, Incident Commander or SWAT Unit Commander may authorize the delivery and use of tear gas, and only after evaluating all conditions known at the time and determining that such force reasonably appears justified and necessary.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Control Devices and Techniques

When practicable, fire personnel should be alerted or summoned to the scene prior to the deployment of tear gas to control any fires and to assist in providing medical aid or gas evacuation if needed.

307.7 OLEORESIN CAPSICUM (OC) GUIDELINES

OLEORESIN CAPSICUM (OC) GUIDELINES

- (a) Oleoresin Capsicum (OC) based aerosol products, will be authorized for use by department members in accordance with this policy.
- (b) This substance is intended for use in situations that do not require the use of deadly force. Using this substance may greatly reduce the need for other types of physical force by the officer, which could result in serious or potentially deadly injury to the offender, officer or others present. The governing factor in the use of the aerosol is whether its use is OBJECTIVELY REASONABLE based on the totality of the circumstances.
- (c) OC-based aerosol products are authorized for use by all officers who meet department training and certification requirements.
- (d) Officers shall carry only department issued canisters. No other product shall be carried or deployed.
- (e) Authorization to use or carry aerosol defensive tools (OC) may be revoked by the officer's supervisor at any time.
- (f) Any use of an OC-based product contrary to the direction of this policy can result in the revocation of the officer's right to use such product and may subject the officer to disciplinary action.

USE OF OC-BASED AEROSOLS

Use of an OC-based product may prevent the use of more severe physical force, and may be used when:

- (a) An officer is threatened with physical force and other means of controlling the offender are unreasonable or could cause more serious injury to the offender, the officer, or others present.
- (b) An officer is threatened by a dangerous animal.
- (c) In cases where the size or demeanor of an offender indicates that the officer or offender would be endangered by the use of other physical force.
- (d) When an officer has articulable circumstances that an offender either verbally or physically expresses non-compliance to the officer's lawful orders.
- (e) Any intentional or accidental use of an OC-based product, except during approved training, will be reported in writing to the officer's supervisor as soon as practical.
- (f) If the use of an OC-based product is accidental, the officer is required to submit a report to his/her immediate supervisor. This documentation will be maintained in the officer's divisional file as well as a copy being forwarded by the officer's supervisor to the appropriate division commander. The following information will be included in the

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Control Devices and Techniques

police first report when an OC-based product is used: 1. All circumstances surrounding the use of the aerosol. 2. Effects on the offender that were caused by the aerosol. 3. Name, address, DOB, and arrest charges for the offender.

- (g) First aid measures given to, or offered to, the offender to neutralize or alleviate the effects of the product.

As with other control devices, oleoresin capsicum (OC) spray and pepper projectiles may be considered for use to bring under control an individual or groups of individuals who are engaging in, or are about to engage in violent behavior. Pepper projectiles and OC spray should not, however, be used against individuals or groups who merely fail to disperse or do not reasonably appear to present a risk to the safety of officers or the public.

307.7.1 OC SPRAY

Uniformed field personnel carrying the oleoresin capsicum (OC) spray shall carry the device in its holster on the equipment belt or on the approved exterior load bearing vest. Plainclothes and non-field personnel may carry the OC spray as authorized, consistent with the needs of their assignment or at the direction of their supervisor. Canisters involved in any type of malfunction or damage shall be turned in to the affected Officers Supervisor for exchange. Damage to City Property forms shall also be forwarded to the appropriate Division Commander and shall explain the cause of damage.

307.7.2 PEPPER PROJECTILE SYSTEMS

Pepper projectiles are plastic spheres that are filled with a derivative of OC powder. Because the compressed gas launcher delivers the projectiles with enough force to burst the projectiles on impact and release the OC powder, the potential exists for the projectiles to inflict injury if they strike the head, neck, spine or groin. Therefore, personnel using a pepper projectile system should not intentionally target those areas, except when the officer reasonably believes the suspect poses an imminent threat of serious bodily injury or death to the officer or others.

Officers encountering a situation that warrants the use of a pepper projectile system shall notify a supervisor as soon as practicable. A supervisor shall respond to all pepper projectile system incidents where the suspect has been hit or exposed to the chemical agent. The supervisor shall ensure that all notifications and reports are completed as required by the Use of Force Policy.

Each deployment of a pepper projectile system shall be documented. This includes situations where the launcher was directed toward the suspect, whether or not the launcher was used. Unintentional discharges shall be promptly reported to a supervisor and documented on the appropriate report form. Only non-incident use of a pepper projectile system, such as training and product demonstrations, is exempt from the reporting requirement.

307.7.3 TREATMENT FOR OC SPRAY EXPOSURE

Anyone exposed to an OC-based product will be afforded decontamination procedures consistent with this policy, if necessary and/or the person is cooperative:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Control Devices and Techniques

- a. Any person exposed to Oleoresin Capsicum (OC) based aerosol products shall be continuously monitored for medical distress while under the care and custody of any member of the South Salt Lake Police Department.
- b. Remove the individual(s) from the contaminated area.
- c. Request medical personnel respond to decontaminate the individual(s).
- d. Flush the affected area with cool water.
- e. Expose the individual(s) to fresh air.
- f. Transport the individual(s) to medical facility for treatment, if necessary.
- g. Once the individual(s) are medically cleared, book the person(s) into jail or take other appropriate actions.
- h. NO individual will be forcibly decontaminated.

307.8 POST-APPLICATION NOTICE

Whenever tear gas or OC has been introduced into a residence, building interior, vehicle or other enclosed area, officers should provide the owners or available occupants with notice of the possible presence of residue that could result in irritation or injury if the area is not properly cleaned. Such notice should include advisement that clean up will be at the owner's expense. Information regarding the method of notice and the individuals notified should be included in related reports.

307.9 OLEORESIN CAPSICUM (OC) DISPOSAL PROCESS

When a unit of Oleoresin Capsicum (OC) reaches its expiration date, it is the officer's responsibility to notify and turn in the OC canister through the Training Sergeant to be properly tracked and disposed. The training Sergeant will enter the expired OC unit in the tracking system updating the status to expired and set for destruction. The Training Sergeant will then turn the expired OC unit into evidence who will handle the destruction of the unit.

307.10 KINETIC ENERGY PROJECTILE GUIDELINES

This department is committed to reducing the potential for violent confrontations. Kinetic energy projectiles, when used properly, are less likely to result in death or serious physical injury and can be used in an attempt to de-escalate a potentially deadly situation.

307.10.1 DEPLOYMENT AND USE

Only department-approved kinetic energy munitions shall be carried and deployed. Approved munitions may be used to compel an individual to cease his/her actions when such munitions present a reasonable option.

Officers are not required or compelled to use approved munitions in lieu of other reasonable tactics if the involved officer determines that deployment of these munitions cannot be done safely. The safety of hostages, innocent persons and officers takes priority over the safety of subjects engaged in criminal or suicidal behavior.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Control Devices and Techniques

Circumstances appropriate for deployment include, but are not limited to, situations in which:

- (a) The suspect is armed with a weapon and the tactical circumstances allow for the safe application of approved munitions.
- (b) The suspect has made credible threats to harm him/herself or others.
- (c) The suspect is engaged in riotous behavior or is throwing rocks, bottles or other dangerous projectiles at people and/or officers.
- (d) There is probable cause to believe that the suspect has already committed a crime of violence and is refusing to comply with lawful orders.

307.10.2 DEPLOYMENT CONSIDERATIONS

Before discharging projectiles, the officer should consider such factors as:

- (a) Distance and angle to target.
- (b) Type of munitions employed.
- (c) Type and thickness of subject's clothing.
- (d) The subject's proximity to others.
- (e) The location of the subject.
- (f) Whether the subject's actions dictate the need for an immediate response and the use of control devices appears appropriate.

A verbal warning of the intended use of the device should precede its application, unless it would otherwise endanger the safety of officers or when it is not practicable due to the circumstances. The purpose of the warning is to give the individual a reasonable opportunity to voluntarily comply and to warn other officers and individuals that the device is being deployed.

Officers should keep in mind the manufacturer's recommendations and their training regarding effective distances and target areas. However, officers are not restricted solely to use according to manufacturer recommendations. Each situation must be evaluated on the totality of circumstances at the time of deployment.

The need to immediately incapacitate the subject must be weighed against the risk of causing serious injury or death. The head and neck should not be intentionally targeted, except when the officer reasonably believes the suspect poses an imminent threat of serious bodily injury or death to the officer or others.

307.11 TRAINING FOR CONTROL DEVICES

The assigned supervisor and/or training sergeant shall ensure that all officers who are authorized to carry a Oleoresin Capsicum (OC) have been properly trained and certified to carry the specific control device and are retrained or recertified as necessary.

- (a) Proficiency training shall be monitored and documented by a certified, control-device weapons or tactics instructor.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Control Devices and Techniques

- (b) All training and proficiency for control devices will be documented in the officer's training file.
- (c) Oleoresin Capsicum (OC) based aerosol voluntary exposure is encouraged for sworn personnel who are fit for duty and wish to carry OC. Contamination during training will help prepare the officer to deal with cross contamination during a realistic encounter. Contamination during training will help prepare the student with the skills to deal with an aerosol irritant projector attack from a violent subject. Contamination during training will help assist the officer in providing evidence during court proceedings. Contamination during training will help assist the officer in understanding proper decontamination.
- (d) Any officer with a pre-existing medical condition as outlined in the SABRE Law Enforcement Instructor manual should not be exposed without prior written authorization from the officers physician. Any officer participating in voluntary OC contamination training shall fill out a voluntary contamination waiver which will be retained in the officer's training file.
- (e) Officers who fail to demonstrate proficiency with the control device or knowledge of this agency's Use of Force Policy will be provided remedial training. If an officer cannot demonstrate proficiency with a control device or knowledge of this agency's Use of Force Policy after remedial training, the officer will be restricted from carrying the control device and may be subject to discipline.

307.12 REPORTING USE OF CONTROL DEVICES AND TECHNIQUES

Any application of a control device or technique listed in this policy shall be documented in the related incident report and reported pursuant to the Use of Force Policy. In the required OC report submission, the brand, manufacture and lot number issued by the South Salt Lake Police Department should be included in the Use of Force Review by the reviewing supervisor.

Conducted Energy Device

308.1 PURPOSE AND SCOPE

This policy provides guidelines for the issuance and use of the conducted energy device (CED).

308.1.1 DEPARTMENT AUTHORIZED ELECTRO-MUSCULAR DISRUPTION TECHNOLOGY DEVICE

Only Electro-Muscular Disruption Technology device; Taser™ Model X26p or Taser 10 will be issued and authorized for use.

308.2 POLICY

The CED is used in an attempt to control a violent or potentially violent individual. The appropriate use of such a device may result in fewer serious injuries to officers and suspects.

308.3 ISSUANCE AND CARRYING CEDS

Only members who have successfully completed [department/office]-approved training may be issued and may carry the CED.

The assigned Training Sergeant shall keep a log of issued CED devices and the serial numbers of cartridges/magazines issued to members.

CEDs are issued for use during a member's current assignment. Those leaving a particular assignment may be required to return the device to the [department/office] inventory.

Officers shall only use the CED and cartridges/magazines that have been issued by the [Department/Office]. Cartridges/magazines should not be used after the manufacturer's expiration date.

Uniformed officers who have been issued the CED shall wear the device in an approved holster.

Officers who carry the CED while in uniform shall carry it in a holster on the side opposite the duty weapon.

- (a) All CEDs shall be clearly distinguishable to differentiate them from the duty weapon and any other device.
- (b) For single-shot devices, whenever practicable, officers should carry an additional cartridge on their person when carrying the CED.
- (c) Officers should not hold a firearm and the CED at the same time.

Non-uniformed officers may secure the CED in a concealed, secure location in the driver's compartment of their vehicles.

308.3.1 FUNCTION OF TASERS

The Taser X26p functions

- (a) It uses compressed nitrogen to project two probes a maximum of 25 feet. An electrical signal is then sent to the probes, via small wires, which temporarily overrides the central nervous system causing temporary muscular incapacitation.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Conducted Energy Device

- (b) The Taser acts as a touch stun system when brought into direct contact with a person's body. When used in this manner the TASER will act as a pain compliance instrument, unless it is used in certain areas of the body, covered in the certification class.

The Taser 10 functions

a. Has 10 probes per cartridge with the ability to individually target each probe for improved accuracy, with a maximum of 45 feet, without the need to reload. An electrical signal is then sent to the probes, via small wires, which temporarily overrides the central nervous system causing temporary muscular incapacitation.

Comparison of various Taser functions.

[See attachment: axon_onepager_taserengeryweaponcomparison_17x11_04a-digital.pdf](#)

308.3.2 TACTICAL CONSIDERATIONS

A. Officers deploying the Taser should have a cover officer whenever possible.

B. Consider the suspect's clothing and probe trajectory when using the weapon. If probes hit clothing, the effects of the Taser may be minimized.

C. The target area should be the subject's center of mass and from behind the subject if possible. Users will not deliberately aim for areas of the face, neck, or groin.

In the diagram below the Blue Shaded areas indicate the preferred areas for Taser deployment. (Note: failure to strike these areas does not indicate a violation of this policy)

D. Officers should consider the presence of cover and distance from the suspect. The probes from the Taser are only effective at distances of 25 feet or less.

E. The Taser is not intended to replace an officer's firearm when deadly force is warranted.

F. Officers should avoid using the Taser on women that are known to be pregnant.

G. Officers should avoid using the Taser on subjects who are on a slanted rooftop, near the edge of buildings or in an elevated position

H. Officers should avoid using the Taser on a subject who is known to be saturated with or in the presence of highly flammable or combustible materials or liquids. As the Taser can easily ignite the combustible material.

I. If deployed on a subject that is attempting to run away, the deploying officer should stay close enough to the subject to keep the probe wires from breaking.

J. Targeted subjects will be restrained as soon as possible. Ideally the subject will be restrained while the Taser cycles.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Conducted Energy Device

308.3.3 USER RESPONSIBILITIES

Officers shall be responsible for ensuring that the issued CED is properly maintained and in good working order. This includes a function test and battery life monitoring, as required by the manufacturer, and should be completed prior to the beginning of the officer's shift.

CEDs that are damaged or inoperative, or cartridges/magazines that are expired or damaged, shall be returned to the Firearms Supervisor for disposition. Officers shall submit documentation stating the reason for the return and how the CED or cartridge/magazine was damaged or became inoperative, if known.

308.4 VERBAL AND VISUAL WARNINGS

A verbal warning of the intended use of the CED should precede its application, unless it would otherwise endanger the safety of officers or when it is not practicable due to the circumstances. The purpose of the warning is to:

- (a) Provide the individual with a reasonable opportunity to voluntarily comply.
- (b) Provide other officers and individuals with a warning that the CED may be deployed.

If, after a verbal warning, an individual fails to voluntarily comply with an officer's lawful orders and it appears both reasonable and feasible under the circumstances, the officer may, but is not required to, activate any warning on the device, which may include display of the electrical arc, an audible warning, or the laser in a further attempt to gain compliance prior to the application of the CED. The laser should not be intentionally directed into anyone's eyes.

The fact that a verbal or other warning was given or the reasons it was not given shall be documented by the officer deploying the CED in the related report.

308.5 USE OF THE CED

The CED has limitations and restrictions requiring consideration before its use. The CED should only be used when its operator can safely deploy the device within its operational range. Although the CED may be effective in controlling most individuals, officers should be aware that the device may not achieve the intended results and be prepared with other options.

If sufficient personnel are available and can be safely assigned, an officer designated as lethal cover for any officer deploying a CED may be considered for officer safety.

308.5.1 APPLICATION OF THE CED

The CED may be used when the circumstances reasonably perceived by the officer at the time indicate that such application reasonably appears necessary to control a person who:

- (a) Is violent or is physically resisting.
- (b) Has demonstrated, by words or action, an intention to be violent or to physically resist, and reasonably appears to present the potential to harm officers, themselves, or others.

Mere flight from a pursuing officer, without additional circumstances or factors, is not good cause for the use of the CED to apprehend an individual.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Conducted Energy Device

The CED shall not be used to psychologically torment, to elicit statements, or to punish any individual.

308.5.2 SPECIAL DEPLOYMENT CONSIDERATIONS

The use of the CED on certain individuals should generally be avoided unless the totality of the circumstances indicates that other available options reasonably appear ineffective or would present a greater danger to the officer, the subject, or others, and the officer reasonably believes that the need to control the individual outweighs the potential risk of using the device. This includes:

- (a) Individuals who are known to be pregnant.
- (b) Elderly individuals or obvious juveniles.
- (c) Individuals with obviously low body mass.
- (d) Individuals who are handcuffed or otherwise restrained.
- (e) Individuals known to have been recently sprayed with a flammable chemical agent or who are otherwise known to be in close proximity to any known combustible vapor or flammable material, including alcohol-based oleoresin capicum (OC) spray.
- (f) Individuals whose position or activity is likely to result in collateral injury (e.g., falls from height, located in water, operating vehicles).

Any CED capable of being applied in the drive-stun mode (i.e., direct contact without probes as a primary form of pain compliance) should be limited to supplementing the probe-mode to complete the circuit, or as a distraction technique to gain separation between officers and the subject, thereby giving officers time and distance to consider other force options or actions.

308.5.3 TARGETING CONSIDERATIONS

Recognizing that the dynamics of a situation and movement of the subject may affect target placement of probes, when practicable, officers should attempt to target the back, lower center mass, and upper legs of the subject, and avoid intentionally targeting the head, neck, area of the heart, or genitals. If circumstances result in one or more probes inadvertently striking an area outside of the preferred target zones, the individual should be closely monitored until examined by paramedics or other medical personnel.

308.5.4 MULTIPLE APPLICATIONS OF THE CED

Once an officer has successfully deployed two probes on the subject, the officer should continually assess the subject to determine if additional probe deployments or cycles reasonably appear necessary. Additional factors officers may consider include but are not limited to:

- (a) Whether it is reasonable to believe that the need to control the individual outweighs the potentially increased risk posed by multiple applications.
- (b) Whether the probes are making proper contact.
- (c) Whether the individual has the ability and has been given a reasonable opportunity to comply.
- (d) Whether verbal commands or other options or tactics may be more effective.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Conducted Energy Device

Given that on certain devices (e.g., TASER 10™) each trigger pull deploys a single probe, the officer must pull the trigger twice to deploy two probes to create the possibility of neuro-muscular incapacitation.

308.5.5 ACTIONS FOLLOWING DEPLOYMENTS

Officers should take appropriate actions to control and restrain the individual as soon as reasonably practicable to minimize the need for longer or multiple exposures to the CED. As soon as practicable, officers shall notify a supervisor any time the CED has been discharged. If needed for evidentiary purposes, the expended cartridge, along with any probes and wire, should be submitted into evidence (including confetti tags, when equipped on the device). The evidence packaging should be marked "Biohazard" if the probes penetrated the subject's skin.

308.5.6 DANGEROUS ANIMALS

The CED may be deployed against an animal if the animal reasonably appears to pose an imminent threat to human safety.

308.5.7 OFF-DUTY CONSIDERATIONS

Officers are not authorized to carry [department/office] CEDs while off-duty.

Officers shall ensure that CEDs are secured while in their homes, vehicles, or any other area under their control, in a manner that will keep the device inaccessible to others.

308.6 DOCUMENTATION

Officers shall document all CED discharges in the related arrest/crime reports and the CED report forms. Photographs should be taken of any obvious probe impact or drive-stun application sites and attached to the CED report form. Notification shall also be made to a supervisor in compliance with the Use of Force Policy. Unintentional discharges, pointing the device at a person, audible warning, laser activation, and arcing the device, other than for testing purposes, will also be documented on the report form (Utah Code 53-13-116; UAC R728-507-12). Data downloads from the CED after use on a subject should be done as soon as practicable using a [department/office]-approved process to preserve the data.

308.6.1 CED REPORT FORM

As applicable based on the device type, items that shall be included in the CED report form are:

- (a) The brand, model, and serial number of the CED and any cartridge/magazine.
- (b) Date, time, and location of the incident.
- (c) Whether any warning, display, laser, or arc deterred a subject and gained compliance.
- (d) The number of probes deployed, CED activations, the duration of each cycle, the duration between activations, and (as best as can be determined) the duration that the subject received applications.
- (e) The range at which the CED was used.
- (f) The type of mode used (e.g., probe deployment, drive-stun).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Conducted Energy Device

- (g) Location of any probe impact.
- (h) Location of contact in drive-stun mode.
- (i) Description of where missed probes went.
- (j) Whether medical care was provided to the subject.
- (k) Whether the subject sustained any injuries.
- (l) Whether any officers sustained any injuries.

The Training Coordinator should periodically analyze the report forms to identify trends, including deterrence and effectiveness. The Training Coordinator should also conduct audits of CED device data downloaded to an approved location and reconcile CED report forms with recorded activations. CED information and statistics, with identifying information removed, should periodically be made available to the public.

308.6.2 REPORTS

The officer should include the following in the arrest/crime report:

- (a) Identification of all personnel firing CEDs
- (b) Identification of all witnesses
- (c) Medical care provided to the subject
- (d) Observations of the subject's physical and physiological actions
- (e) Any known or suspected drug use, intoxication, or other medical problems

308.7 MEDICAL TREATMENT

Consistent with local medical personnel protocols and absent extenuating circumstances, only appropriate medical personnel should remove CED probes from a person's body. Used CED probes shall be treated as a sharps biohazard, similar to a used hypodermic needle, and handled appropriately. Universal precautions should be taken.

All persons who have been struck by CED probes, who have been subjected to the electric discharge of the device, or who sustained direct exposure of the laser to the eyes shall be medically assessed prior to booking. Additionally, any such individual who falls under any of the following categories should, as soon as practicable, be examined by paramedics or other qualified medical personnel:

- (a) The person is suspected of being under the influence of controlled substances and/or alcohol.
- (b) The person may be pregnant.
- (c) The person reasonably appears to be in need of medical attention.
- (d) The CED probes are lodged in a sensitive area (e.g., groin, female breast, head, face, neck).
- (e) The person requests medical treatment.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Conducted Energy Device

Any individual exhibiting signs of distress or who is exposed to multiple or prolonged applications shall be transported to a medical facility for examination or medically evaluated prior to booking. If any individual refuses medical attention, such a refusal should be witnessed by another officer and/or medical personnel and shall be fully documented in related reports. If an audio/video recording is made of the contact or an interview with the individual, any refusal should be included, if possible.

The transporting officer shall inform any person providing medical care or receiving custody that the individual has been subjected to the application of the CED (see the Medical Aid and Response Policy).

308.8 SUPERVISOR RESPONSIBILITIES

When possible, supervisors should respond to calls when they reasonably believe there is a likelihood the CED may be used. A supervisor should respond to all incidents where the CED was activated.

A supervisor should review each incident where a person has been exposed to a CED. The device's internal logs should be downloaded by a supervisor or Firearms Supervisor and saved with the related arrest/crime report. The supervisor should arrange for photographs of probe sites to be taken and witnesses to be interviewed.

308.9 TRAINING

Personnel who are authorized to carry the CED shall be permitted to do so only after successfully completing the initial [department/office]-approved training. Any personnel who have not carried the CED as a part of their assignments for a period of six months or more shall be recertified by a qualified CED instructor prior to again carrying or using the device.

Proficiency training for personnel who have been issued CEDs should occur every year. A reassessment of an officer's knowledge and/or practical skills may be required at any time, if deemed appropriate, by the Training Coordinator. All training and proficiency for CEDs will be documented in the officer's training files.

Command staff, supervisors, and investigators should receive CED training as appropriate for the investigations they conduct and review.

Officers who do not carry CEDs should receive training that is sufficient to familiarize them with the device and with working with officers who use the device.

The Training Coordinator is responsible for ensuring that all members who carry CEDs have received initial and annual proficiency training. Periodic audits should be used for verification.

Application of CEDs during training could result in injuries and should not be mandatory for certification.

The Training Coordinator should include the following training:

- (a) A review of this policy.
- (b) A review of the Use of Force Policy.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Conducted Energy Device

- (c) Performing weak-hand draws or cross-draws until proficient to reduce the possibility of unintentionally drawing and firing a firearm.
- (d) Target area considerations, to include techniques or options to reduce the unintentional application of probes to the head, neck, area of the heart, and groin.
- (e) Scenario-based training, including virtual reality training when available.
- (f) Handcuffing a subject during the application of the CED and transitioning to other force options.
- (g) De-escalation techniques.
- (h) Restraint techniques that do not impair respiration following the application of the CED.
- (i) Proper use of cover and concealment during deployment of the CED for purposes of officer safety.
- (j) Proper tactics and techniques related to multiple applications of CEDs.

308.10 CONTROL AND INVENTORY OF ALL EMDT DEVICES

309.7.1 CONTROL AND INVENTORY OF ALL EMDT DEVICES

All Taser's™ will be issued an asset tag by the EMDT Coordinator.

The EMDT Coordinator will record the asset tag number, serial number of the Taser device and the name of the officer issued that particular Taser, into the inventory system.

It is the EMDT Coordinator's responsibility to issue Taser's to officers and keep accurate records regarding the Taser inventory, assignment, deployment, return, and re-issue.

No Taser will be issued to an officer until it has been properly recorded as described above.

Once a Taser has been issued to an officer, the Taser will not be turned over to another officer unless or until directed to do so by the EMDT Coordinator, and that information is recorded in the Taser inventory system.

Returning a Taser to the EMDT Coordinator:

As with all equipment and weapons, when an officer is transferred to an assignment that is not authorized for a Taser, or an officer leaves the employment of the South Salt Lake Police Department, the issued Taser will be returned to the EMDT Coordinator.

The EMDT Coordinator will enter the new status of the Taser into the inventory system.

Handcuffing and Restraints

309.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of handcuffs and other restraints during detentions and arrests.

309.2 POLICY

The South Salt Lake Police Department authorizes the use of restraint devices in accordance with this policy, the Use of Force Policy, the Transporting Persons in Custody Policy, and [department/office] training. Restraint devices shall not be used to punish, to display authority, or as a show of force (Utah Code 77-7-1).

309.3 USE OF RESTRAINTS

Only members who have successfully completed South Salt Lake Police Department-approved training on the use of restraint devices described in this policy are authorized to use these devices.

When deciding whether to use any restraint, officers should carefully balance officer safety concerns with factors that include, but are not limited to:

- The circumstances or crime leading to the arrest.
- The demeanor and behavior of the arrested person.
- The age and health of the person.
- Whether the person is known to be pregnant.
- Whether the person has a hearing or speaking disability. In such cases, consideration should be given, safety permitting, to handcuffing to the front in order to allow the person to sign or write notes.
- Whether the person has any other apparent disability.

309.3.1 RESTRAINT OF DETAINEES

Situations may arise where it may be reasonable to restrain an individual who may, after brief investigation, be released without arrest. Unless arrested, the use of restraints on detainees should continue only for as long as is reasonably necessary to assure the safety of officers and others. When deciding whether to remove restraints from a detainee, officers should continuously weigh the safety interests at hand against the continuing intrusion upon the detainee.

309.3.2 RESTRAINT OF PREGNANT PERSONS

Persons who are known to be pregnant should be restrained in the least restrictive manner that is effective for officer safety. Leg restraints, waist chains, or handcuffs behind the body should not be used unless the officer has a reasonable suspicion that the person may resist, attempt escape, injure themselves or others, or damage property.

No person who is in labor, delivery, or recovery after delivery shall be handcuffed or restrained except in extraordinary circumstances, and only when a supervisor makes an individualized

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Handcuffing and Restraints

determination that such restraints are necessary for the safety of the detainee, officers, or others. See the Transporting Persons in Custody Policy for guidelines relating to transporting pregnant persons.

309.3.3 RESTRAINT OF JUVENILES

A juvenile under 14 years of age should not be restrained unless he/she is suspected of a dangerous felony or when the officer has a reasonable suspicion that the juvenile may resist, attempt escape, injure him/herself, injure the officer or damage property.

309.4 APPLICATION OF HANDCUFFS OR PLASTIC CUFFS

Handcuffs, including temporary nylon or plastic cuffs, may be used only to restrain a person's hands to ensure officer safety.

Although recommended for most arrest situations, handcuffing is discretionary and not an absolute requirement of the [Department/Office]. Officers should consider handcuffing any person they reasonably believe warrants that degree of restraint. However, officers should not conclude that in order to avoid risk every person should be handcuffed, regardless of the circumstances.

In most situations handcuffs should be applied with the hands behind the person's back. When feasible, handcuffs should be double-locked to prevent tightening, which may cause undue discomfort or injury to the hands or wrists.

In situations where one pair of handcuffs does not appear sufficient to restrain the individual or may cause unreasonable discomfort due to the person's size, officers should consider alternatives, such as using an additional set of handcuffs or multiple plastic cuffs.

Handcuffs should be removed as soon as it is reasonable or after the person has been searched and is safely confined within a detention facility.

309.5 APPLICATION OF SPIT HOODS/MASKS/SOCKS

Spit hoods/masks/socks are temporary protective devices designed to prevent the wearer from biting and/or transferring or transmitting fluids (saliva and mucous) to others.

Spit hoods may be placed upon persons in custody when the officer reasonably believes the person will bite or spit, either on a person or in an inappropriate place. They are generally used during application of a physical restraint, while the person is restrained, or during or after transport.

Officers utilizing spit hoods should ensure that the spit hood is fastened properly to allow for adequate ventilation and that the restrained person can breathe normally. Officers should provide assistance during the movement of restrained individuals due to the potential for impaired or distorted vision on the part of the individual. Officers should avoid comingling individuals wearing spit hoods with other detainees.

Spit hoods should not be used in situations where the restrained person is bleeding profusely from the area around the mouth or nose, or if there are indications that the person has a medical condition, such as difficulty breathing or vomiting. In such cases, prompt medical care should be obtained. If the person vomits while wearing a spit hood, the spit hood should be promptly removed.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Handcuffing and Restraints

and discarded. Persons who have been sprayed with oleoresin capsicum (OC) spray should be thoroughly decontaminated including hair, head and clothing prior to application of a spit hood.

Those who have been placed in a spit hood should be continually monitored and shall not be left unattended until the spit hood is removed. Spit hoods shall be discarded after each use.

309.6 APPLICATION OF AUXILIARY RESTRAINT DEVICES

Auxiliary restraint devices include transport belts, waist or belly chains, transportation chains, leg restraints, and other similar devices. Auxiliary restraint devices are intended for use during long-term restraint or transportation. They provide additional security and safety without impeding breathing, while permitting adequate movement, comfort, and mobility.

Only [department/office]-authorized devices may be used. Any person in auxiliary restraints should be monitored as reasonably appears necessary. The South Salt Lake Police Department authorizes the use of the BODY WRAP as an auxiliary restraint device. The use of the auxiliary restraint device may only be utilized by an officer only after the initial introduction course is completed and recertification is current.

309.7 APPLICATION OF LEG RESTRAINT DEVICES

Leg restraints may be used to restrain the legs of a violent or potentially violent person when it is reasonable to do so during the course of detention, arrest, or transportation. Only restraint devices approved by the [Department/Office] shall be used.

In determining whether to use the leg restraint, officers should consider:

- (a) Whether the officer or others could be exposed to injury due to the assaultive or resistant behavior of a suspect.
- (b) Whether it is reasonably necessary to protect the suspect from their own actions (e.g., hitting their head against the interior of the patrol unit, running away from the arresting officer while handcuffed, kicking at objects or officers).
- (c) Whether it is reasonably necessary to avoid damage to property (e.g., kicking at windows of the patrol unit).

309.7.1 GUIDELINES FOR USE OF LEG RESTRAINTS

When applying leg restraints, the following guidelines should be followed:

- (a) If practicable, officers should notify a supervisor of the intent to apply the leg restraint device. In all cases, a supervisor shall be notified as soon as practicable after the application of the leg restraint device.
- (b) Once applied, absent a medical or other emergency, restraints should remain in place until the officer arrives at the jail or other facility or the person no longer reasonably appears to pose a threat.
- (c) Once secured, the person should be placed in a seated or upright position, secured with a seat belt, and shall not be placed on their stomach for an extended period, as this could reduce the person's ability to breathe.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Handcuffing and Restraints

- (d) The restrained person should be continually monitored by an officer while in the leg restraint. The officer should ensure that the person does not roll onto and remain on their stomach.
- (e) The officer should look for signs of labored breathing and take appropriate steps to relieve and minimize any obvious factors contributing to this condition.

309.8 REQUIRED DOCUMENTATION

If a person is restrained and released without an arrest, the officer shall document the details of the detention and the need for handcuffs or other restraints.

If a person is arrested, the use of handcuffs or other restraints shall be documented in the related report.

Officers should document the following information in reports, as appropriate, when restraints other than handcuffs are used on a person:

- (a) The factors that led to the decision to use restraints.
- (b) Supervisor notification and approval of restraint use.
- (c) The types of restraint used.
- (d) The amount of time the suspect was restrained.
- (e) How the person was transported and the position of the person during transport.
- (f) Observations of the person's behavior and any signs of physiological problems.
- (g) Any known or suspected drug use or other medical problems.

309.9 TRAINING

The Training Coordinator should ensure that officers receive periodic training on the proper use of handcuffs and other restraints, including:

- (a) Proper placement and fit of handcuffs and other restraint devices approved for use by the [Department/Office].
- (b) Response to complaints of pain by restrained persons.
- (c) Options for restraining those who may be pregnant without the use of leg restraints, waist chains, or handcuffs behind the body.
- (d) Options for restraining amputees or those with medical conditions or other physical conditions that may be aggravated by being restrained.
- (e) Proper placement of safely secured persons into an upright or seated position to avoid placement on the stomach for an extended period, as this could reduce the person's ability to breathe.
- (f) Training for the auxiliary restraint system (Body Wrap) will include the 2 hour introduction course and every two year recertification. Officers are not authorized to use the Body Wrap until training is completed and current.

Firearms

310.1 PURPOSE AND SCOPE

This policy provides guidelines for issuing firearms, the safe and legal carrying of firearms, firearms maintenance, and firearms training.

This policy does not apply to issues related to the use of firearms that are addressed in the Use of Force or Officer-Involved Shootings and Deaths policies.

This policy only applies to those members who are authorized to carry firearms.

310.2 POLICY

The South Salt Lake Police Department will equip its members with firearms to address the risks posed to the public and [department/office] members by violent and sometimes well-armed persons. The [Department/Office] will ensure firearms are appropriate and in good working order and that relevant training is provided as resources allow.

310.3 AUTHORIZED FIREARMS, AMMUNITION, AND OTHER WEAPONS

Members shall only use firearms that are issued or approved by the [Department/Office] and have been thoroughly inspected by the Firearms Supervisor. Except in an emergency or as directed by a supervisor, no firearm shall be carried by a member who has not qualified with that firearm at an authorized [department/office] range.

All other weapons not provided by the [Department/Office], including but not limited to edged weapons, chemical or electronic weapons, impact weapons, or any weapon prohibited or restricted by law or that is not covered elsewhere by [department/office] policy, may not be carried by members in the performance of their official duties without the express written authorization of the member's Division Commander. This exclusion does not apply to the carrying of a single folding pocketknife that is not otherwise prohibited by law.

310.3.1 HANDGUNS

The authorized [department/office]-issued handgun is the Glock 17 9mm. The following additional handguns are approved for on-duty use:

MAKE	MODEL	CALIBER

310.3.2 PATROL RIFLES

The authorized department-issued patrol rifle is the AR15 (Style) and H&K UMP.

Members may deploy the patrol rifle in any circumstance where the member can articulate a reasonable expectation that the rifle may be needed. Examples of some general guidelines for deploying the patrol rifle may include, but are not limited to:

- (a) Situations where the member reasonably anticipates an armed encounter.
- (b) When a member is faced with a situation that may require accurate and effective fire at long range.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Firearms

- (c) Situations where a member reasonably expects the need to meet or exceed a suspect's firepower.
- (d) When a member reasonably believes that there may be a need to fire on a barricaded person or a person with a hostage.
- (e) When a member reasonably believes that a suspect may be wearing body armor.
- (f) When authorized or requested by a supervisor.
- (g) When needed to euthanize an animal.

When not deployed, the patrol rifle shall be properly secured consistent with department training in a locking weapons rack or locked trunk in the patrol vehicle. The patrol rifle in unmarked police vehicles will be secured in a locked trunk or installed rifle/gun lock box.

310.3.3 PERSONALLY OWNED DUTY FIREARMS

Members desiring to carry an authorized but personally owned duty firearm must receive written approval from the Chief of Police or the authorized designee. Once approved, personally owned duty firearms are subject to the following restrictions:

- (a) The firearm shall be in good working order and on the [department/office] list of approved firearms.
- (b) The firearm shall be inspected by the Firearms Supervisor prior to being carried and thereafter shall be subject to inspection whenever it is deemed necessary.
- (c) Prior to carrying the firearm, members shall qualify under range supervision and thereafter shall qualify in accordance with the [department/office] qualification schedule. Members must demonstrate proficiency and safe handling, and that the firearm functions properly.
- (d) Members shall provide written notice of the make, model, color, serial number, and caliber of the firearm to the Firearms Supervisor, who will maintain a list of the information.

310.3.4 AUTHORIZED SECONDARY HANDGUN

Members desiring to carry [department/office] or personally owned secondary handguns are subject to the following restrictions:

- (a) The handgun shall be in good working order and on the [department/office] list of approved firearms.
- (b) Only one secondary handgun may be carried at a time.
- (c) The purchase of the handgun and ammunition shall be the responsibility of the member unless the handgun and ammunition are provided by the [Department/Office].
- (d) The handgun shall be carried concealed at all times and in such a manner as to prevent unintentional cocking, discharge, or loss of physical control.
- (e) The handgun shall be inspected by the Firearms Supervisor prior to being carried and thereafter shall be subject to inspection whenever it is deemed necessary.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Firearms

- (f) Ammunition shall be the same as [department/office] issue. If the caliber of the handgun is other than [department/office] issue, the Chief of Police or the authorized designee shall approve the ammunition.
- (g) Prior to carrying the secondary handgun, members shall qualify under range supervision and thereafter shall qualify in accordance with the [department/office] qualification schedule. Members must demonstrate proficiency and safe handling, and that the handgun functions properly.
- (h) Members shall provide written notice of the make, model, color, serial number, and caliber of a secondary handgun to the Firearms Supervisor, who will maintain a list of the information.

310.3.5 AUTHORIZED OFF-DUTY FIREARMS

The carrying of firearms by members while off-duty is permitted by the Chief of Police but may be rescinded should circumstances dictate (e.g., administrative leave). Members who choose to carry a firearm while off-duty, based on their authority as peace officers, will be required to meet the following guidelines:

- (a) A personally owned firearm shall be used, carried, and inspected in accordance with the Personally Owned Duty Firearms requirements in this policy.
 - 1. The purchase of the personally owned firearm and ammunition shall be the responsibility of the member.
- (b) The firearm shall be carried concealed at all times and in such a manner as to prevent unintentional cocking, discharge, or loss of physical control.
- (c) It will be the responsibility of the member to submit the firearm to the Firearms Supervisor for inspection prior to being personally carried. Thereafter the firearm shall be subject to periodic inspection by the Firearms Supervisor.
- (d) Prior to carrying any off-duty firearm, the member shall demonstrate to the Firearms Supervisor that the member is proficient in handling and firing the firearm and that it will be carried in a safe manner.
- (e) The member will successfully qualify with the firearm prior to it being carried.
- (f) Members shall provide written notice of the make, model, color, serial number, and caliber of the firearm to the Firearms Supervisor, who will maintain a list of the information.
- (g) If a member desires to use more than one firearm while off-duty, the member may do so, as long as all requirements set forth in this policy for each firearm are met.
- (h) Members shall only carry [department/office]-authorized ammunition.
- (i) When armed, officers shall carry their badges and South Salt Lake Police Department identification cards under circumstances requiring possession of such identification.

310.3.6 AMMUNITION

Members shall carry only [department/office]-authorized ammunition. Members shall be issued fresh duty ammunition in the specified quantity for all [department/office]-issued firearms during

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Firearms

the member's firearms qualification. Replacements for unserviceable or depleted ammunition issued by the [Department/Office] shall be dispensed by the Firearms Supervisor when needed, in accordance with established policy.

Members carrying personally owned authorized firearms of a caliber differing from [department/office]-issued firearms shall be responsible for obtaining fresh duty ammunition in accordance with the above, at their own expense.

310.4 EQUIPMENT

Firearms carried on- or off-duty shall be maintained in a clean, serviceable condition. Maintenance and repair of authorized personally owned firearms are the responsibility of the individual member.

310.4.1 REPAIRS OR MODIFICATIONS

Each member shall be responsible for promptly reporting any damage or malfunction of an assigned firearm to a supervisor or the Firearms Supervisor.

Firearms that are the property of the Department or personally owned firearms that are approved for department use may be repaired or modified only by a person who is department-approved and certified as an armorer or gunsmith in the repair of the specific firearm. Such modification or repair must be authorized in advance by the Firearms Supervisor.

Any repairs or modifications to the member's personally owned firearm shall be done at his/her expense and must be approved by the Firearms Supervisor.

310.4.2 HOLSTERS

Only [department/office]-approved holsters shall be used and worn by members. Members shall periodically inspect their holsters to make sure they are serviceable and provide the proper security and retention of the handgun.

310.4.3 TACTICAL LIGHTS

Tactical lights may only be installed on a firearm carried on- or off-duty after they have been examined and approved by the Firearms Supervisor. Once the approved tactical lights have been properly installed on any firearm, the member shall qualify with the firearm to ensure proper functionality and sighting of the firearm prior to carrying it.

310.4.4 OPTICS OR LASER SIGHTS

Optics may only be installed on a rifle after they have been examined and approved by the Firearms Supervisor. Any approved sight shall only be installed in strict accordance with manufacturer specifications. Once approved sights have been properly installed on any firearm, the member shall qualify with the firearm to ensure proper functionality and sighting of the firearm prior to carrying it.

Laser Sights are not approved or authorized for handguns or rifles.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Firearms

310.5 SAFE HANDLING, INSPECTION, AND STORAGE

Members shall maintain the highest level of safety when handling firearms and shall consider the following:

- (a) Members shall not unnecessarily display or handle any firearm.
- (b) Members shall be governed by all rules and regulations pertaining to the use of the range and shall obey all orders issued by the Firearms Supervisor. Members shall not dry fire or practice quick draws except as instructed by the Firearms Supervisor or other firearms training staff.
- (c) Members shall not clean, repair, load, or unload a firearm anywhere in the [Department/Office], except where clearing barrels are present.
- (d) Shotguns or rifles removed from vehicles or the equipment storage room shall be loaded and unloaded in the parking lot and outside of the vehicle, using clearing barrels.
- (e) Members shall not place or store any firearm or other weapon on [department/office] premises except where the place of storage is locked. No one shall carry firearms into the jail section or any part thereof when securing or processing an arrestee, but shall place all firearms in a secured location. Members providing access to the jail section to persons from outside agencies are responsible for ensuring firearms are not brought into the jail section.
- (f) Members shall not use any automatic firearm, heavy caliber rifle, gas, or other type of chemical weapon or firearm from the armory, except with approval of a supervisor.
- (g) Any firearm authorized by the [Department/Office] to be carried on- or off-duty that is determined by a member to be malfunctioning or in need of service or repair shall not be carried. It shall be promptly presented to the [Department/Office] or a Firearms Supervisor approved by the [Department/Office] for inspection and repair. Any firearm deemed in need of repair or service by the Firearms Supervisor will be immediately removed from service. If the firearm is the member's primary duty firearm, a replacement firearm will be issued to the member until the duty firearm is serviceable.

310.5.1 INSPECTION AND STORAGE

Handguns and rifles shall be inspected regularly and upon access or possession by another person. The member shall ensure that the firearm is carried in the proper condition and loaded with approved ammunition. Inspection of rifle shall be done while standing outside of the patrol vehicle. All firearms shall be pointed in a safe direction or into clearing barrels.

Personally owned firearms may be safely stored in lockers at the end of the shift. Department-owned firearms shall be stored in the appropriate equipment storage room. Handguns may remain loaded if they are secured in an appropriate holster. Rifles shall be unloaded in a safe manner outside the building and then stored in the appropriate equipment storage room.

310.5.2 STORAGE AT HOME

Members shall ensure that all firearms and ammunition are locked and secured while in their homes, vehicles or any other area under their control, and in a manner that will keep them

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Firearms

inaccessible to children and others who should not have access. Members shall not permit [department/office]-issued firearms to be handled by anyone not authorized by the [Department/Office] to do so. Members should be aware that negligent storage of a firearm could result in civil liability.

310.5.3 ALCOHOL AND DRUGS

Firearms shall not be carried by any member, either on- or off-duty, who has consumed an amount of an alcoholic beverage, taken any drugs or medication, or has taken any combination thereof that would tend to adversely affect the member's senses or judgment.

310.6 FIREARMS TRAINING AND QUALIFICATIONS

All members who carry a firearm while on-duty are required to successfully complete training with their duty firearms. All members will qualify at least twice during the training year with their duty firearm, issued rifle, off-duty and secondary firearms.

At least annually, all members carrying a firearm should receive practical training designed to simulate field situations including low-light shooting.

310.6.1 NON-CERTIFICATION OR NON-QUALIFICATION

If any member fails to meet minimum standards for firearms training or qualification for any reason, including injury, illness, duty status or scheduling conflict, that member shall submit a memorandum to his/her immediate supervisor prior to the end of the required training or qualification period.

Those who fail to meet minimum standards or qualify on their first shooting attempt shall be provided remedial training and will be subject to the following requirements:

- (a) Additional range assignments may be scheduled to assist the member in demonstrating consistent firearm proficiency.
- (b) Members shall be given credit for a range training or qualification when obtaining a qualifying score or meeting standards after remedial training.
- (c) No range credit will be given for the following:
 - 1. Unauthorized range make-up
 - 2. Failure to meet minimum standards or qualify after remedial training

Members who repeatedly fail to meet minimum standards will be removed from field assignment and may be subject to disciplinary action.

310.6.2 REQUIREMENTS PRIOR TO CARRYING

Before being authorized to carry a firearm, officers shall be issued copies of, and demonstrate understanding of, this policy and the Use of Force Policy.

310.7 FIREARM DISCHARGE

Except during training or recreational use, any member who discharges a firearm intentionally or unintentionally, on- or off-duty, shall make a verbal report to his/her supervisor as soon as

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Firearms

circumstances permit. If the discharge results in injury or death to another person, additional statements and reports shall be made in accordance with the Officer-Involved Shootings and Deaths Policy. If a firearm was discharged as a use of force, the involved member shall adhere to the additional reporting requirements set forth in the Use of Force Policy.

In all other cases, written reports shall be made as follows:

- (a) If on-duty at the time of the incident, the member shall file a written report with his/her Division Commander or provide a recorded statement to investigators prior to the end of shift, unless otherwise directed.
- (b) If off-duty at the time of the incident, a written report shall be submitted or a recorded statement provided no later than the end of the next regularly scheduled shift, unless otherwise directed by a supervisor.

310.7.1 DESTRUCTION OF ANIMALS

Members are authorized to use firearms to stop an animal in circumstances where the animal reasonably appears to pose an imminent threat to human safety and alternative methods are not reasonably available or would likely be ineffective.

In circumstances where there is sufficient advance notice that a potentially dangerous animal may be encountered, [department/office] members should develop reasonable contingency plans for dealing with the animal (e.g., fire extinguisher, conducted energy device, oleoresin capsicum (OC) spray, animal control officer). Nothing in this policy shall prohibit any member from shooting a dangerous animal if circumstances reasonably dictate that a contingency plan has failed, becomes impractical, or if the animal reasonably appears to pose an imminent threat to human safety.

310.7.2 INJURED ANIMALS

With the approval of a supervisor, a member may euthanize an animal that is so badly injured that human compassion requires its removal from further suffering and where other dispositions are impractical. Before destroying the animal, the officer shall obtain either the judgment of a veterinarian or of two reputable citizens called by the officer to view the animal in the presence of the officer, or shall obtain consent to the destruction from the owner of the animal (Utah Code 76-13-102(4)).

310.7.3 WARNING AND OTHER SHOTS

Generally, shots fired for the purpose of summoning aid are discouraged and may not be discharged unless the member reasonably believes that they appear necessary, effective, and reasonably safe.

Warning shots shall not be used.

310.8 FIREARMS SUPERVISOR DUTIES

The range will be under the exclusive control of the Firearms Supervisor. All members attending will follow the directions of the Firearms Supervisor. The Firearms Supervisor will maintain a roster of all members attending the range and will submit the roster to the Training Coordinator after

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Firearms

each range date. Failure of any officer to sign in and out with the Firearms Supervisor may result in non-qualification.

The range shall remain operational and accessible to [department/office] members during hours established by the [Department/Office].

The Firearms Supervisor has the responsibility of making periodic inspection, at least once a year, of all duty weapons carried by officers of the [department/office] to verify proper operation. The Firearms Supervisor has the authority to deem any privately owned weapon unfit for service. The officer will be responsible for all repairs to their personally owned weapon, and it will not be returned to service until inspected by the Firearms Supervisor.

The Firearms Supervisor has the responsibility for ensuring each member meets the minimum requirements during training shoots and, on at least a yearly basis, can demonstrate proficiency in the care, cleaning, and safety of all firearms the member is authorized to carry.

The Firearms Supervisor shall complete and submit to the Training Coordinator documentation of the training courses provided. Documentation shall include the qualifications of each instructor who provides the training, a description of the training provided and, on a form that has been approved by the [Department/Office], a list of each member who completes the training. The Firearms Supervisor should keep accurate records of all training shoots, qualifications, repairs, maintenance, or other records as directed by the Training Coordinator.

310.9 FLYING WHILE ARMED

The Transportation Security Administration (TSA) has imposed rules governing law enforcement officers flying armed on commercial aircraft. The following requirements apply to officers who intend to be armed while flying on a commercial air carrier or flights where screening is conducted (49 CFR 1544.219):

- (a) Officers wishing to fly while armed must be flying in an official capacity, not for vacation or pleasure, and must have a need to have the firearm accessible, as determined by the [Department/Office] based on the law and published TSA rules.
- (b) Officers must carry their South Salt Lake Police Department identification card, bearing the officer's name, a full-face photograph, identification number, the officer's signature, and the signature of the Chief of Police or the official seal of the [Department/Office], and must present this identification to airline officials when requested. The officer should also carry the standard photo identification needed for passenger screening by airline and TSA officials (e.g., driver license, passport).
- (c) The South Salt Lake Police Department must submit a National Law Enforcement Telecommunications System (NLETS) message prior to the officer's travel. If approved, TSA will send the South Salt Lake Police Department an NLETS message containing a unique alphanumeric identifier. The officer must present the message on the day of travel to airport personnel as authorization to travel while armed.
- (d) An official letter signed by the Chief of Police authorizing armed travel may also accompany the officer. The letter should outline the officer's need to fly armed, detail

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Firearms

their itinerary, and should include that the officer has completed the mandatory TSA training for a law enforcement officer flying while armed.

- (e) Officers must have completed the mandated TSA security training covering officers flying while armed. The training shall be given by the [department/office]-appointed instructor.
- (f) It is the officer's responsibility to notify the air carrier in advance of the intended armed travel. This notification should be accomplished by early check-in at the carrier's check-in counter.
- (g) Any officer flying while armed should discreetly contact the flight crew prior to take-off and notify them of the officer's assigned seat.
- (h) Discretion must be used to avoid alarming passengers or crew by displaying a firearm. The officer must keep the firearm concealed on their person at all times. Firearms are not permitted in carry-on luggage and may not be stored in an overhead compartment.
- (i) Officers should try to resolve any problems associated with flying armed through the flight captain, ground security manager, TSA representative, or other management representative of the air carrier.
- (j) Officers shall not consume alcoholic beverages while aboard an aircraft, or within eight hours prior to boarding an aircraft.

310.10 CARRYING FIREARMS OUT OF STATE

Qualified, active, full-time officers of this [department/office] are authorized to carry a concealed firearm in all other states subject to the following conditions (18 USC § 926B):

- (a) The officer shall carry their South Salt Lake Police Department identification card whenever carrying such firearm.
- (b) The officer is not the subject of any current disciplinary action.
- (c) The officer may not be under the influence of alcohol or any other intoxicating or hallucinatory drug.
- (d) The officer will remain subject to this and all other [department/office] policies (including qualifying and training).

Officers are cautioned that individual states may enact local regulations that permit private persons or entities to prohibit or restrict the possession of concealed firearms on their property, or that prohibit or restrict the possession of firearms on any state or local government property, installation, building, base, or park. Federal authority may not shield an officer from arrest and prosecution in such locally restricted areas.

Active law enforcement officers from other states are subject to all requirements set forth in 18 USC § 926B.

Domestic Violence

311.1 PURPOSE AND SCOPE

The purpose of this policy is to provide the guidelines necessary to deter, prevent, and reduce domestic violence through vigorous enforcement and to address domestic violence as a serious crime against society. The policy specifically addresses the commitment of this [department/office] to take enforcement action when appropriate, to provide assistance to victims, and to guide officers in the investigation of domestic violence.

311.1.1 DEFINITIONS

Definitions related to this policy include:

Court order - All forms of orders related to domestic and dating violence, that have been issued by a court of this state or another, whether civil or criminal, regardless of whether service has been made.

Dating violence - Any criminal offense involving violence or physical harm, threat of violence or physical harm, or any attempt, conspiracy, or solicitation by a person to commit an offense involving violence or physical harm, when committed by a person against a dating partner of the person who is either 18 years of age or older or is emancipated (Utah Code 78B-7-102).

Domestic violence - Includes any crime involving the actual, threatened, or attempted violence or physical harm of a cohabitant. Domestic violence also includes committing or attempting to commit any crime listed in Utah Code 77-36-1 by one cohabitant against another.

311.2 POLICY

The South Salt Lake Police Department's response to incidents of domestic violence and violations of related court orders shall stress enforcement of the law to protect the victim and shall communicate the philosophy that domestic violence is criminal behavior. It is also the policy of this [department/office] to facilitate victims' and offenders' access to appropriate civil remedies and community resources whenever feasible.

311.3 OFFICER SAFETY

The investigation of domestic violence cases often places officers in emotionally charged and sometimes highly dangerous environments. No provision of this policy is intended to supersede the responsibility of all officers to exercise due caution and reasonable care in providing for the safety of any officers and parties involved.

311.4 INVESTIGATIONS

The following guidelines should be followed by officers when investigating domestic violence cases:

- (a) Calls of reported, threatened, imminent, or ongoing domestic violence and the violation of any court order are of extreme importance and should be considered among the

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Domestic Violence

highest response priorities. This includes incomplete 9-1-1 calls. Writing a police report (General Offense Report) are required on all Domestic Violence calls for service.

- (b) When practicable, officers should obtain and document statements from the victim, the suspect, and any witnesses, including children, in or around the household or location of occurrence.
- (c) Officers should list the full name and date of birth (and school if available) of each child who was present in the household at the time of the offense. The names of other children who may not have been in the house at that particular time should also be obtained for follow-up.
- (d) When practicable and legally permitted, video or audio record all significant statements and observations.
- (e) All injuries should be photographed, regardless of severity, taking care to preserve the victim's personal privacy. Where practicable, photographs should be taken by a person of the same sex. Victims whose injuries are not visible at the time of the incident should be asked to contact the Investigations Division in the event that the injuries later become visible.
- (f) Officers should request that the victim complete and sign an authorization for release of medical records related to the incident when applicable.
- (g) If the suspect is no longer at the scene, officers should make reasonable efforts to locate the suspect to further the investigation, provide the suspect with an opportunity to make a statement, and make an arrest or seek an arrest warrant if appropriate.
- (h) Seize any firearms or other dangerous weapons in the home, if appropriate and legally permitted, for safekeeping or as evidence.
 - 1. This applies to both investigations involving domestic violence or dating violence (Utah Code 77-36-2.1; Utah Code 78B-7-408).
- (i) When completing an incident or arrest report for violation of a court order, officers should include specific information that establishes that the offender has been served, including the date the offender was served, the name of the agency that served the order, and the provision of the order that the subject is alleged to have violated. When reasonably available, the arresting officer should attach a copy of the order to the incident or arrest report.
- (j) Officers shall take appropriate enforcement action when there is probable cause to believe an offense has occurred. Factors that should not be used as sole justification for declining to take enforcement action include:
 - 1. Whether the suspect lives on the premises with the victim.
 - 2. Claims by the suspect that the victim provoked or perpetuated the violence.
 - 3. The potential financial or child custody consequences of arrest.
 - 4. The physical or emotional state of either party.
 - 5. Use of drugs or alcohol by either party.
 - 6. Denial that the abuse occurred where evidence indicates otherwise.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Domestic Violence

7. A request by the victim not to arrest the suspect.
 8. Location of the incident (public/private).
 9. Speculation that the complainant may not follow through with the prosecution.
 10. Actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, disability, or marital status of the victim or suspect.
 11. The social status, community status, or professional position of the victim or suspect.
- (k) If the offense is alleged against an intimate partner, the officers shall conduct a lethality assessment as required by Utah Code 77-36-2.1. The lethality assessment shall be recorded on the appropriate form and the results submitted to the Department of Public Safety while on scene or as soon as reasonably practicable (Utah Code 77-36-2.1).
- (l) [Utah State Code 77-36-2.1 Duties of Law Enforcement Officers](#)

311.4.1 IF A SUSPECT IS ARRESTED

If a suspect is arrested, officers should:

- (a) Advise the victim that there is no guarantee the suspect will remain in custody.
- (b) Provide the victim's contact information to the jail staff to enable notification of the victim upon the suspect's release from jail.
- (c) Advise the victim whether any type of court order will be in effect when the suspect is released from jail.

311.4.2 IF NO ARREST IS MADE

If no arrest is made, the officer should:

- (a) Advise the parties of any options, including but not limited to:
 1. Voluntary separation of the parties.
 2. Appropriate resource referrals (e.g., counselors, friends, relatives, shelter homes, victim witness assistance).
- (b) Document the resolution in a report.

311.5 VICTIM ASSISTANCE

Because victims may be traumatized or confused, officers should be aware that a victim's behavior and actions may be affected. The following applies to domestic violence and dating violence (Utah Code 77-36-2.1; Utah Code 78B-7-408):

- (a) Officers who respond to allegations of domestic violence shall use all reasonable means to protect the victim and prevent further violence.
- (b) Victims shall be provided with the [Department/Office]'s domestic violence information handout, even if the incident may not rise to the level of a crime.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Domestic Violence

- (c) Victims shall also be alerted to any available victim advocates, shelters, and community resources and advised of the results of the lethality assessment if applicable.
- (d) When an involved person requests law enforcement assistance while removing essential items of personal property, officers shall stand by for a reasonable amount of time.
- (e) If the victim has sustained injury or complains of pain, the officer shall seek medical assistance for the victim as soon as practicable.
- (f) Officers should ask the victim whether the victim has a safe place to stay and assist in arranging transportation to an alternate shelter if the victim expresses a concern for the victim's safety or if the officer determines that a need exists.
- (g) Officers should make reasonable efforts to ensure that any children or dependent adults who are under the supervision of the suspect or victim are being properly cared for.
- (h) If appropriate, officers shall seek or assist the victim in obtaining an emergency order.
- (i) When applicable, the victim should be provided with the required information from the Department of Public Safety regarding the right to voluntarily turn over a firearm to a law enforcement agency for safekeeping.

311.5.1 VICTIM ASSISTANCE UNIT CALL-OUT OR NOTIFICATION

- (a) The on-call victim advocate shall be notified anytime a victim of domestic violence is transported to the hospital or indicates they are going to seek medical attention. This will allow the victim advocate the opportunity to respond and meet with the victim to discuss a safety plan, seek safe shelter and/or receive information about "Crime Victim Reparations" who may pay for medical treatment.
- (b) The on-call victim advocate should be contacted anytime the officer is unsure what assistance can or should be offered to the victim.
- (c) The on-call victim advocate should be contacted anytime the score on the mandatory lethality assessment is considered high risk.
- (d) Regardless of whether contact is made with the on-call victim advocate or not, the officer will always provide the victim with a "South Salt Lake Victim Assistance Program" pamphlet and information about a Domestic Violence Service provider referral (YWCA).

311.6 DISPATCH ASSISTANCE

All calls of domestic violence, including incomplete 9-1-1 calls, should be dispatched as soon as practicable.

Dispatchers are not required to verify the validity of a court order before responding to a request for assistance. Officers should request that dispatchers check whether any of the involved persons are subject to the terms of a court order.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Domestic Violence

311.7 FOREIGN COURT ORDERS

Various types of orders may be issued in domestic violence cases. Any foreign court order properly issued by a court of another state, Indian tribe or territory shall be enforced by officers as if it were the order of a court in this state. An order should be considered properly issued when it reasonably appears that the issuing court has jurisdiction over the parties and reasonable notice and opportunity to respond was given to the party against whom the order was issued (18 USC § 2265). An otherwise valid out-of-state court order shall be enforced, regardless of whether the order has been properly registered with this state.

311.7.1 CANADIAN DOMESTIC VIOLENCE PROTECTION ORDERS

If there is probable cause to believe a valid Canadian domestic violence protection order exists and has been violated, an officer shall enforce the terms of the order as if it were the order of a court in this state (Utah Code 78B-7-1202).

311.8 VERIFICATION OF COURT ORDERS

Determining the validity of a court order, particularly an order from another jurisdiction, can be challenging. Therefore, in determining whether there is probable cause to make an arrest for a violation of any court order, officers should carefully review the actual order when available, and, where appropriate and practicable:

- (a) Ask the subject of the order about his/her notice or receipt of the order, his/her knowledge of its terms and efforts to respond to the order.
- (b) Check available records or databases that may show the status or conditions of the order.
- (c) Contact the issuing court to verify the validity of the order.
- (d) Contact a law enforcement official from the jurisdiction where the order was issued to verify information.

Officers should document in an appropriate report their efforts to verify the validity of an order, regardless of whether an arrest is made. Officers should contact a supervisor for clarification when needed.

311.9 LEGAL MANDATES AND RELEVANT LAWS

Utah law provides for the following:

311.9.1 STANDARDS FOR ARRESTS

- (a) Officers responding to a domestic violence call shall arrest or issue a citation to a domestic violence offender if there is probable cause to believe an offense has occurred. The offense need not occur in the officer's presence (Utah Code 77-36-2.2). Any citation issued shall note that the offense involved a domestic violence offense (Utah Code 77-7-20).
- (b) An officer shall arrest an alleged perpetrator whenever there is probable cause to believe that the alleged perpetrator has violated any of the provisions of a court order or condition of release agreement and there is evidence the order has been served.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Domestic Violence

The offense need not occur in the officer's presence (Utah Code 77-36-2.4; Utah Code 78B-7-119).

- (c) If an officer has probable cause to believe there will be continued violence against the victim or if there is evidence that the perpetrator has either recently caused serious bodily injury or used a dangerous weapon in the domestic violence offense, the officer may not utilize the option of issuing a citation (Utah Code 77-36-2.2). Factors that may support the likelihood of a continuing offense include:
 - 1. A prior history of arrests or citations involving domestic violence.
 - 2. The alleged perpetrator is violating a court order.
 - 3. The alleged perpetrator has a prior history of other assaultive behavior (e.g., arrests or convictions for assault and battery or aggravated assaults).
 - 4. The victim states that the alleged perpetrator has a history of physical abuse toward the victim.
 - 5. The victim expresses fear of retaliation or further violence should the alleged perpetrator be released.
 - 6. Any other evidence that would indicate the victim may be subjected to continued violence or abuse.
- (d) In responding to domestic violence incidents, officers should generally be reluctant to make dual arrests. If an officer receives complaints of domestic violence from two or more opposing persons, the officer shall evaluate each complaint separately to identify the predominant physical aggressor. If the officer determines that one person was the predominant physical aggressor, the officer need not arrest the other person alleged to have committed domestic violence. In determining the predominant aggressor, the officer shall consider (Utah Code 77-36-2.2):
 - 1. Any prior complaints of domestic violence.
 - 2. The relative severity of injuries inflicted on each person.
 - 3. The likelihood of future injury to each of the parties.
 - 4. Whether one of the parties acted in self-defense.
- (e) An officer may not threaten, suggest, or otherwise indicate the possible arrest of all parties in order to discourage any party's request for intervention by law enforcement (Utah Code 77-36-2.2).
- (f) Whenever an alleged perpetrator is arrested or issued a citation and subsequently released by this [department/office], the releasing officer shall then make a reasonable effort to notify the victim of that release and shall transmit that information to the statewide domestic violence network (Utah Code 78B-7-802).
- (g) An officer who does not make an arrest shall notify the victim of their right to initiate a criminal proceeding and of the importance of preserving evidence (Utah Code 77-36-2.2).
- (h) Whenever a complainant advises of the existence of a court order, the officer shall determine if a valid court order exists and use every reasonable means to enforce

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Domestic Violence

the order. The officer should determine whether the order is in the statewide domestic violence network (Utah Code 78B-7-113) and/or:

1. Whether a court order is on file with a law enforcement agency or whether the complainant has a copy of the court order in their possession.
 2. Whether proof of service or prior notice exists, whether the alleged perpetrator was in court when the order was made, or it was provided by a court ex parte.
 3. The terms of the court order that may be enforced against the alleged perpetrator.
- (i) In the event the alleged perpetrator is no longer at the scene, officers shall document the incident for follow-up investigation.
- (j) If an arrest is made or a citation is issued, the arresting officer shall provide the individual with written notice containing the following information (Utah Code 78B-7-802):
1. The individual may not telephone, contact, or otherwise communicate directly or indirectly with the victim before being released.
 2. The individual may not be released except by court order or a written jail release agreement.
 3. Notification of the penalties for violation of the court order or any jail release agreement executed and that the individual must appear in court on the next business day after arrest.

311.9.2 REPORTS AND RECORDS

- (a) Reports on all incidents of domestic violence shall include (Utah Code 77-36-2.2):
1. The officer's disposition of the case.
 2. The appropriate crime classification for domestic violence.
 3. If no arrest was made, the report shall detail the grounds for not arresting.
 4. If two parties are arrested, the report shall detail the grounds for arresting both parties.
 5. The results of a lethality assessment when required by Utah Code 77-36-2.1. The report, however, shall not reflect information about a referral to a domestic violence organization if one is made as a result of the lethality assessment.
- (b) The officer creating the report should provide the victim with the case number of the report. The case number may be placed in the appropriate space on the victim information handout provided to the victim. If the case number is not immediately available, the officer should explain to the victim how the victim can obtain the information at a later time.
- (c) The report shall be made available to the victim, upon request, at no cost (Utah Code 77-36-2.2(6)(d)).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Domestic Violence

- (d) The Records Supervisor shall forward a copy of the incident report to the appropriate prosecuting attorney within five days after the complaint of domestic violence occurred (Utah Code 77-36-2.2(6)(c)).
- (e) The officer completing a domestic violence report should include information regarding whether the victim would like the court to impose release restrictions upon the arrestee, including prohibiting the arrestee from having personal contact with the victim or from entering the victim's residence or other premises temporarily occupied by the victim (Utah Code 78B-7-802).
- (f) The Records Supervisor or the authorized designee shall update the statewide domestic violence network when a person is released upon a written jail release agreement (Utah Code 78B-7-802; Utah Code 78B-7-113).

311.10 SERVICE OF COURT ORDERS

When an officer serves an individual with a protective order which causes the individual to be a restricted person under Utah Code 76-11-302 or Utah Code 76-11-303, the officer shall verbally provide the individual with the appropriate firearm restriction notifications in accordance with Utah Code 76-11-309 and request the individual's signature on the acknowledgment contained within the protective order document.

Officer-Involved Shootings and Deaths

313.1 PURPOSE AND SCOPE

The purpose of this policy is to establish policy and procedures for the investigation of an incident in which a person is injured or dies as the result of an officer-involved shooting or dies as a result of other action of an officer.

In other incidents not covered by this policy, the Chief of Police may decide that the investigation will follow the process provided in this policy.

313.2 INVESTIGATION RESPONSIBILITY

This department conforms to the Salt Lake County District Attorney Officer Involved Shooting Protocol for investigating officer-involved shootings.

313.3 TYPES OF INVESTIGATIONS

Officer-involved shootings involve several separate investigations. The investigations may include:

- (a) A criminal investigation of the incident by the agency having jurisdiction where the incident occurred. This department may relinquish its criminal investigation to an outside agency with the approval of the Chief of Police or a Division Commander.
- (b) A criminal investigation of the involved officer(s) conducted by an outside agency.
- (c) A civil investigation to determine potential liability conducted by the involved officer's agency.
- (d) An administrative investigation conducted by the involved officer's agency to determine if there were any violations of any Department policy.

313.4 CONTROL OF INVESTIGATIONS

Investigators from Officer Involved Critical Incident Protocol Team (OICI) may be assigned to work on the criminal investigation of officer-involved shootings and deaths. This may include at least one investigator from the agency that employs the involved officer.

Jurisdiction is determined by the location of the shooting or death and the agency employing the involved officer. The following scenarios outline the jurisdictional responsibilities for investigating officer-involved shootings and deaths.

313.4.1 SOUTH SALT LAKE POLICE DEPARTMENT OFFICER WITHIN THIS JURISDICTION

The South Salt Lake Police Department is responsible for the criminal investigation of the suspect's actions, the civil investigation and the administrative investigation. The criminal investigation of the officer-involved shooting will be conducted by the Officer Involved Critical Incident Protocol Team (OICI)

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Officer-Involved Shootings and Deaths

313.4.2 ALLIED AGENCY'S OFFICER WITHIN THIS JURISDICTION

The South Salt Lake Police Department is responsible for the criminal investigation of the suspect's actions. The criminal investigation of the officer-involved shooting will be conducted by the Officer Involved Critical Incident Protocol Team.. The officer's employing agency will be responsible for any civil and/or administrative investigation(s).

313.4.3 SOUTH SALT LAKE POLICE DEPARTMENT OFFICER IN ANOTHER JURISDICTION

The agency where the incident occurred has criminal jurisdiction and is responsible for the criminal investigation of the incident. That agency may relinquish its criminal investigation of the suspect(s) to another agency. The South Salt Lake Police Department will conduct timely civil and/or administrative investigations.

313.4.4 INVESTIGATION RESPONSIBILITY MATRIX

The following table identifies the possible scenarios and responsibilities for the investigation of officer-involved shootings.

	Criminal Investigation of Suspect(s)	Criminal Investigation of Officer(s)	Administrative Investigation
SSLPD Officer in This Jurisdiction	SSLPD Investigators or OICI		SSLPD Internal Affairs Unit
Allied Agency's Officer in This Jurisdiction	SSLPD Investigators or OICI		Involved Officer's Department
SSLPD Officer in Another Jurisdiction	Agency where incident occurred	Decision made by agency where incident occurred	SSLPD Internal Affairs Unit

313.5 INVESTIGATION PROCESS

The following procedures are guidelines used in the investigation of an officer-involved shooting or death.

313.5.1 UNINVOLVED OFFICER RESPONSIBILITIES

Upon arrival at the scene of an officer-involved shooting or death, the first uninvolved SSLPD officer will be the Incident Commander and will assume the responsibilities of a supervisor until properly relieved. This officer should, as appropriate:

- (a) Secure the scene and identify and eliminate hazards for all those involved.
- (b) Take reasonable steps to obtain emergency medical attention for injured individuals.
- (c) Request additional resources from the Department or other agencies.
- (d) Coordinate a perimeter or pursuit of suspects.
- (e) Check for injured persons and evacuate as needed.
- (f) Brief the supervisor upon arrival.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Officer-Involved Shootings and Deaths

313.5.2 SUPERVISOR RESPONSIBILITIES

Upon arrival at the scene, the first uninvolved SSLPD supervisor should ensure completion of the duties as outlined above, plus:

- (a) Attempt to obtain a brief overview of the situation from any uninvolved officers.
 1. In the event that there are no uninvolved officers who can supply adequate overview, the supervisor should attempt to obtain a brief voluntary overview from one involved officer.
- (b) If necessary, the supervisor may administratively order any SSLPD officer to immediately provide public safety information necessary to secure the scene, identify injured parties and pursue suspects.
 1. Public safety information shall be limited to such things as outstanding suspect information, number and direction of any shots fired, perimeter of the incident scene, identity of known or potential witnesses and any other pertinent information.
 2. The initial on-scene supervisor should not attempt to order any involved officer to provide any information other than public safety information.
- (c) Provide all available information to the Watch Commander and Dispatch. If feasible, sensitive information should be communicated over secure networks.
- (d) Take command of and secure the incident scene with additional SSLPD members until properly relieved by another supervisor or other assigned personnel or investigator.
- (e) As soon as practicable, ensure that involved officers are transported (separately, if feasible) to a suitable location for further direction.
 1. Each involved SSLPD officer should be given an administrative order not to discuss the incident with other involved officers or SSLPD members pending further direction from a supervisor.
 2. When an involved officer's weapon is taken or left at the scene for other than officer-safety reasons (e.g., evidence), ensure that he/she is provided with a comparable replacement weapon or transported by other officers.

313.5.3 WATCH COMMANDER RESPONSIBILITIES

Upon learning of an officer-involved shooting or death, the Watch Commander shall be responsible for coordinating all aspects of the incident until he/she is relieved by the Chief of Police or a Division Commander.

All outside inquiries about the incident shall be directed to the Watch Commander.

313.5.4 NOTIFICATIONS

The following persons shall be notified as soon as practicable:

- Chief of Police
- Investigation Division Commander
- Salt Lake County District Attorney Officer Involved Critical Incident Protocol Team.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Officer-Involved Shootings and Deaths

- Outside agency investigators (if appropriate)
- Professional Standards Unit supervisor
- Civil liability response team
- Psychological/peer support personnel
-
- Medical Examiner (if necessary)
- Involved officer's agency representative (if requested)
- Public Information Officer
- District Attorney (Utah Code 76-2-408)

313.5.5 INVOLVED OFFICERS

The following shall be considered for the involved officer:

- (a) Any request for legal or union representation will be accommodated.
 - 1. Involved SSLPD officers shall not be permitted to meet collectively or in a group with an attorney or any representative prior to providing a formal interview or report.
 - 2. Requests from involved non-SSLPD officers should be referred to their employing agency.
- (b) Discussions with licensed attorneys will be considered privileged as attorney-client communications.
- (c) Discussions with agency representatives/employee groups will be privileged only as to the discussion of non-criminal information.
- (d) A licensed psychotherapist shall be provided by the Department to each involved SSLPD officer. A licensed psychotherapist may also be provided to any other affected SSLPD members, upon request.
 - 1. Interviews with a licensed psychotherapist will be considered privileged.
 - 2. An interview or session with a licensed psychotherapist may take place prior to the member providing a formal interview or report. However, involved members shall not be permitted to consult or meet collectively or in a group with a licensed psychotherapist prior to providing a formal interview or report.
 - 3. A separate fitness-for-duty exam may also be required (see the Fitness for Duty Policy).
- (e) Communications with a peer support team member will be considered privileged to the extent provided in Utah Code 78B-5-903.

Care should be taken to preserve the integrity of any physical evidence present on the involved officer's equipment or clothing, such as blood or fingerprints, until investigators or lab personnel can properly retrieve it.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Officer-Involved Shootings and Deaths

Each involved SSLPD officer shall be given reasonable paid administrative leave following an officer-involved shooting or death. It shall be the responsibility of the Watch Commander to make schedule adjustments to accommodate such leave.

313.6 CRIMINAL INVESTIGATION

The Officer Involved Critical Incident Protocol Team is responsible for the criminal investigation into the circumstances of any officer-involved shooting or death.

If available, investigative personnel from this department may be assigned to partner with investigators from outside agencies or the District Attorney's Office to avoid duplicating efforts in related criminal investigations.

Once public safety issues have been addressed, criminal investigators should be given the opportunity to obtain a voluntary statement from involved officers and to complete their interviews. The following shall be considered for the involved officer:

- (a) SSLPD supervisors and Professional Standards Unit personnel should not participate directly in any voluntary interview of SSLPD officers. This will not prohibit such personnel from monitoring interviews or providing the criminal investigators with topics for inquiry.
- (b) If requested, any involved officer will be afforded the opportunity to consult individually with a representative of his/her choosing or an attorney prior to speaking with criminal investigators. However, in order to maintain the integrity of each involved officer's statement, involved officers shall not consult or meet with a representative or an attorney collectively or in groups prior to being interviewed.
- (c) If any involved officer is physically, emotionally or otherwise not in a position to provide a voluntary statement when interviewed by criminal investigators, consideration should be given to allowing a reasonable period for the officer to schedule an alternate time for the interview.
- (d) Any voluntary statement provided by an involved officer will be made available for inclusion in any related investigation, including administrative investigations. However, no administratively coerced statement will be provided to any criminal investigators unless the officer consents.

313.6.1 REPORTS BY INVOLVED SSLPD OFFICERS

In the event that suspects remain outstanding or subject to prosecution for related offenses, this department shall retain the authority to require involved SSLPD officers to provide sufficient information for related criminal reports to facilitate the apprehension and prosecution of those individuals.

While the involved SSLPD officers may write the report, it is generally recommended that such reports be completed by assigned investigators, who should interview all involved officers as victims/witnesses. Since the purpose of these reports will be to facilitate criminal prosecution, statements of involved officers should focus on evidence to establish the elements of criminal

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Officer-Involved Shootings and Deaths

activities by suspects. Care should be taken not to duplicate information provided by involved officers in other reports.

Nothing in this section shall be construed to deprive an involved SSLPD officer of the right to consult with legal counsel prior to completing any such criminal report.

Reports related to the prosecution of criminal suspects will be processed according to normal procedures but should also be included for reference in the investigation of the officer-involved shooting or death.

313.6.2 WITNESS IDENTIFICATION AND INTERVIEWS

Because potential witnesses to an officer-involved shooting or death may become unavailable or the integrity of their statements compromised with the passage of time, a supervisor should take reasonable steps to promptly coordinate with criminal investigators to utilize available law enforcement personnel for the following:

- (a) Identification of all persons present at the scene and in the immediate area.
 - 1. When feasible, a recorded statement should be obtained from those persons who claim not to have witnessed the incident but who were present at the time it occurred.
 - 2. Any potential witness who is unwilling or unable to remain available for a formal interview should not be detained absent reasonable suspicion to detain or probable cause to arrest. Without detaining the individual for the sole purpose of identification, attempts to identify the witness prior to his/her departure should be made whenever feasible.
- (b) Witnesses who are willing to provide a formal interview should be asked to meet at a suitable location where criminal investigators may obtain a recorded statement. Such witnesses, if willing, may be transported by a member of the Department.
 - 1. A written, verbal or recorded statement of consent should be obtained prior to transporting a witness. When the witness is a minor, consent should be obtained from the parent or guardian, if available, prior to transportation.
- (c) Promptly contacting the suspect's known family and associates to obtain any available and untainted background information about the suspect's activities and state of mind prior to the incident.

313.6.3 INVESTIGATIVE PERSONNEL

Once notified of an officer-involved shooting or death, it shall be the responsibility of the designated Investigations Division supervisor to assign appropriate investigative personnel to handle the investigation of related crimes. Department investigators will be assigned to work with investigators from the OICI Team and may be assigned to separately handle the investigation of any related crimes not being investigated by the OICI Team.

All related department reports, except administrative and/or privileged reports, will be forwarded to the designated Investigations Division supervisor for approval. Privileged reports shall be

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Officer-Involved Shootings and Deaths

maintained exclusively by members who are authorized such access. Administrative reports will be forwarded to the appropriate Division Commander.

313.7 ADMINISTRATIVE INVESTIGATION

In addition to all other investigations associated with an officer-involved shooting or death, this department will conduct an internal administrative investigation to determine conformance with all department policy. This investigation will be conducted under the supervision of the Professional Standards Unit and will be considered a confidential officer personnel file.

Interviews of members shall be subject to department policies and applicable laws.

- (a) Any officer involved in a shooting or death may be requested or administratively compelled to provide a blood sample for alcohol/drug screening. Absent consent from the officer, such compelled samples and the results of any such testing shall not be disclosed to any criminal investigative agency.
- (b) If any officer has voluntarily elected to provide a statement to criminal investigators, the assigned administrative investigator should review that statement before proceeding with any further interview of that involved officer.
 - 1. If a further interview of the officer is deemed necessary to determine policy compliance, care should be taken to limit the inquiry to new areas with minimal, if any, duplication of questions addressed in the voluntary statement. The involved officer shall be provided with a copy of his/her prior statement before proceeding with any subsequent interviews.
- (c) In the event that an involved officer has elected not to provide criminal investigators with a voluntary statement, the assigned administrative investigator shall conduct an administrative interview to determine all relevant information.
 - 1. Although this interview should not be unreasonably delayed, care should be taken to ensure that the officer's physical and psychological needs have been addressed before commencing the interview.
 - 2. If requested, the officer shall have the opportunity to select an uninvolved representative to be present during the interview. However, in order to maintain the integrity of each individual officer's statement, involved officers shall not consult or meet with a representative or attorney collectively or in a group prior to being interviewed.
 - 3. Administrative interviews should be recorded by the investigator. The officer may also record the interview.
 - 4. The officer shall be informed of the nature of the investigation. If an officer refuses to answer questions, he/she should be given his/her *Garrity* rights and ordered to provide full and truthful answers to all questions. The officer shall be

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Officer-Involved Shootings and Deaths

informed that the interview will be for administrative purposes only and that the statement cannot be used criminally.

5. The Professional Standards Unit shall compile all relevant information and reports necessary for the Department to determine compliance with applicable policies.
6. Regardless of whether the use of force is an issue in the case, the completed administrative investigation shall be submitted to the Use of Force Review Board, which will restrict its findings as to whether there was compliance with the Use of Force Policy.
7. Any other indications of a potential violation of any policy shall be determined in accordance with standard disciplinary procedures.

313.8 AUDIO AND VIDEO RECORDINGS

Any officer involved in an incident may be permitted to review available Mobile Audio Video (MAV) or other video or audio recordings prior to providing a recorded statement or completing reports.

Upon request, non-law enforcement witnesses who are able to verify their presence and their ability to contemporaneously perceive events at the scene of an incident may also be permitted to review available MAV or other video or audio recordings with approval of assigned investigators or a supervisor.

Any MAV and other known video or audio recordings of an incident should not be publicly released during an ongoing investigation without consulting the prosecuting attorney or City Attorney's Office as appropriate.

313.9 DEBRIEFING

Following an officer-involved shooting or death, the South Salt Lake Police Department should conduct both a critical incident/stress debriefing and a tactical debriefing.

313.9.1 CRITICAL INCIDENT/STRESS DEBRIEFING

A critical incident/stress debriefing should occur as soon as practicable. The Administration Division Commander is responsible for organizing the debriefing. Notes and recorded statements should not be taken because the sole purpose of the debriefing is to help mitigate the stress-related effects of a traumatic event.

The debriefing is not part of any investigative process. Care should be taken not to release or repeat any communication made during a debriefing unless otherwise authorized by policy, law or a valid court order.

Attendance at the debriefing shall only include those members of the Department directly involved in the incident, which can include support personnel (e.g., dispatcher, other non-sworn). Family or other support personnel may attend with the concurrence of those involved in the incident. The debriefing shall be closed to the public and should be closed to all other members of the Department, including supervisory and Professional Standards Unit personnel.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Officer-Involved Shootings and Deaths

313.9.2 TACTICAL DEBRIEFING

A tactical debriefing should take place to identify any training or areas of policy that need improvement. The Chief of Police should identify the appropriate participants. This debriefing should not be conducted until all involved members have provided recorded or formal statements to criminal and/or administrative investigators.

313.10 MEDIA RELATIONS

Any media release shall be prepared with input and concurrence from the supervisor and department representative responsible for each phase of the investigation. Releases will be available to the Watch Commander, Investigation Division Commander and Public Information Officer in the event of inquiries from the media.

No involved SSLPD officer shall make any comment to the media unless he/she is authorized by the Chief of Police or a Division Commander.

Department members receiving inquiries regarding officer-involved shootings or deaths occurring in other jurisdictions shall refrain from public comment and will direct those inquiries to the agency having jurisdiction and primary responsibility for the investigation.

Victim and Witness Assistance

314.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure that crime victims and witnesses receive appropriate assistance, that they are provided with information from government and private resources, and that the agency meets all related legal mandates.

314.2 POLICY

The South Salt Lake Police Department is committed to providing guidance and assistance to the victims and witnesses of crime. The employees of the South Salt Lake Police Department will show compassion and understanding for victims and witnesses and will make reasonable efforts to provide the support and information identified in this policy.

314.3 CRIME VICTIMS

Officers should provide all victims with the applicable victim information handouts.

Officers should never guarantee a victim's safety from future harm but may make practical safety suggestions to victims who express fear of future harm or retaliation. Officers should never guarantee that a person qualifies as a victim for the purpose of compensation or restitution but may direct him/her to the proper written department material or available victim resources.

314.4 INVESTIGATIVE ASSISTANCE

- (a) During the preliminary investigation of any incident the responding officer(s) or victim advocate will, as the need indicates:
 - 1. Provide the victim/witness with information about applicable services, e.g., counseling, medical attention, compensation programs, and victim advocacy.
 - 2. Advise the victim/witness about what to do if the suspect, suspects companion, or family threatens or otherwise intimidates him/her.
 - 3. Provide the incident case number.
 - 4. Provide an avenue for reporting additional information about the case or to receive information about the case.
- (b) During the follow-up investigation, the investigator or victim advocate will provide the victim/witness with the following services:
 - 1. If, in the opinion of the agency, the impact of a crime on a victim/witness has been unusually severe and has triggered above-average victim/witness assistance, re-contacting the victim/witness periodically to determine whether needs are being met.
 - 2. If not an endangerment to the successful prosecution of the case, explaining to victims/witnesses the procedures involved in the prosecution of their cases and their role in those procedures.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Victim and Witness Assistance

3. If feasible, scheduling line-ups, interviews, and other required appearances at the convenience of the victim/witness and, at the option of the agency, providing transportation.
 4. If feasible, returning promptly victim/witness property taken as evidence (except for contraband, disputed property, and weapons used in the course of the crime), where permitted by law or rules of evidence.
 5. If needed, assigning a victim advocate to the victim/witness during follow-up investigation.
- (c) Victim / Witness contact after suspect arrest:
1. The investigator and/or victim advocate may provide notification to the victim/witness as of the suspects arrest, charges, and custody status and changes.
 2. Notification may be done only if time, case load, personnel, and availability of information permits.

314.5 VICTIM INFORMATION

The Victim Advocate Supervisor shall ensure that victim information handouts are available and current. These should include as appropriate:

- (a) Shelters and other community resources for victims of domestic violence.
- (b) Community resources for victims of sexual assault (Utah Code 53-10-804).
- (c) Assurance that sexual assault victims will not incur out-of-pocket expenses for forensic medical exams, and information about evidence collection, storage, and preservation in sexual assault cases (34 USC § 10449; 34 USC § 20109).
- (d) An advisement that a person who was arrested may be released on bond or some other form of release and that the victim should not rely upon an arrest as a guarantee of safety.
- (e) A clear explanation of relevant court orders and how they can be obtained.
- (f) Information regarding available compensation for qualifying victims of crime.
- (g) VINE® information (Victim Information and Notification Everyday), including the telephone number and whether this free service is available to allow victims to check on an offender's custody status and to register for automatic notification when a person is released from jail.
- (h) Notice regarding U visa and T visa application processes.
- (i) Resources available for victims of identity theft.
- (j) A place for the officer's name, badge number, and any applicable case or incident number.
- (k) The written notices for victims of domestic violence and other qualifying offenses as mandated by Utah Code 78B-7-802 and Utah Code 77-36-2.1.
- (l) Local victim centers.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Victim and Witness Assistance

- (m) The Utah Department of Corrections (UDC) Victim Services Unit, which can provide assistance and support to victims whose victimizers are in the custody of the UDC.
- (n) Office of Crime Victim Reparations Program that offers financial assistance.
- (o) The Federal Department of Justice Office for Victims of Crime (OVC), which can also provide assistance.
- (p) The Utah Crime Victims' Bill of Rights (Utah Code 77-37-3).
- (q) Rights and remedies available to victims of stalking or dating violence (Utah Code 76-5-106.5; Utah Code 78B-7-408).
- (r) Eligibility and process to request review of investigations (Utah Code 11-64-101).
- (s) The written notices for victims of sexual violence as mandated by Utah Code 78B-7-509.
- (t) A guide for victims of sexual assault to be published on the [Department/Office] website as mandated by Utah Code 53-25-201.

314.6 VICTIM ADVOCATE SUPERVISOR

The Chief of Police should appoint a member of the Department to serve as the victim advocate supervisor. The victim advocate supervisor will be the point of contact for officers and/or individuals requiring further assistance or information from the South Salt Lake Police Department regarding benefits from crime victim resources. The victim advocate supervisor shall also be responsible for maintaining compliance with all legal mandates related to crime victims and/or witnesses. The victim advocate supervisor will be responsible for all grant processing, reporting and submission. The victim advocate supervisor will report to the Investigation Lieutenant.

314.7 VICTIM ADVOCATE/CRIME VICTIM LIAISON DUTIES

The victim advocate/crime victim liaison processes requests to review open investigations as set forth in Utah Code 11-64-101 (Victim Rights Amendments).

The victim advocate/ crime victim liaison shall work with the Utah Office for Victims of Crime to provide information sufficient to determine a claimant's eligibility for a reparations award pursuant to Utah Code 63M-7-527.

314.8 WITNESSES

Officers should never guarantee a witness's safety from future harm or that his/her identity will always remain confidential. Officers may make practical safety suggestions to witnesses who express fear of future harm or retaliation.

Officers should investigate allegations of witness intimidation and take enforcement action when lawful and reasonable.

314.9 VICTIM ASSISTANCE EMERGENCY FUNDS DISBURSEMENT POLICY

The Victim Advocate Supervisor and Administrative Assistant will oversee and administer the receipt and disbursement of funds.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Victim and Witness Assistance

The Victim Advocate Supervisor shall maintain custody of the cash funds and disburse funds to victims as needed. A ledger indicating the date, amount, vendor, purpose and victim recipient of all disbursed funds. Funds may only be used for victim emergency assistance purposes.

A cash balance of \$500 will be maintained for emergency disbursement purposes

A vendor generated receipt is required to support all disbursement of funds.

At any given time the sum of cash and receipts shall be \$500.

The Administrative Assistant will periodically request and approve a disbursement check from the finance department. The check request will be supported by copies of vendor generated receipts and will be in the amount to bring the disbursement account to the \$500 level.

At least weekly (or more often if necessary) the Victim Advocate Supervisor will audit the "on hand" cash, receipts, and ledger to verify proper disbursement and recording of disbursement of victim emergency funds.

314.10 VICTIM ASSISTANCE FOR STALKING

Officers investigating allegations of stalking should take reasonable steps to protect the victim and any family or household member. This includes the following (Utah Code 76-5-106.5):

- (a) Victims shall be provided with the South Salt Lake Police Department stalking information handout, even if the incident may not rise to the level of a crime.
- (b) Victims shall also be alerted to any available victim advocates, shelters, and community resources.
- (c) When an involved person requests law enforcement assistance while removing essential items of personal property, officers shall stand by for a reasonable amount of time.
- (d) If the victim has sustained injury or complains of pain, officers shall seek medical assistance for the victim as soon as practicable.
- (e) Officers should ask the victim whether he/she has a safe place to stay and assist in arranging transportation to an alternate shelter if the victim expresses a concern for his/her safety or if the officer determines that a need exists.
- (f) Officers should make reasonable efforts to ensure that any children or dependent adults who are under the supervision of the suspect or victim are being properly cared for.
- (g) If appropriate, officers shall seek or assist the victim in obtaining an emergency order.
- (h) Seize any firearms or other dangerous weapons, if appropriate and legally permitted, for safekeeping or as evidence.

314.11 DEATH OR SERIOUS INJURY NOTIFICATIONS

- (a) The notification of the next of kin of deceased, seriously injured, or ill persons is carried out in a prompt, professional, and courteous manner, notifications will fall into three categories:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Victim and Witness Assistance

1. Notifications generated by incidents occurring within the South Salt Lake City limits.
 - (a) Death notification will generally be handled by and/or coordinated through the detective division.
 - (b) Notification of local relatives of serious injury persons within South Salt Lake City should be conducted in person, if at all possible.
 - (c) Notifications where there are only minor injuries involved (generally those which are not going to require in-patient medical care) can be conducted by phone.
 - (d) These can be completed by an officer or through the department's communications center, at an officer's request.
 2. Notifications reported to this department from another law enforcement agency, governmental agency, medical facility or doctor, or relative located outside the immediate area.
 - (a) Department personnel will make every effort to deliver notifications, initiated by other agencies, in person.
 - (b) Officers should normally not make any notifications as requested from parties whose identity cannot be otherwise confirmed, without approval of the shift supervisor.
- (b) General
- (a) In cases involving death notification, whenever possible, this notification should be conducted by a police officer and a member of the victim assistance unit..
 - (b) Officers will attempt to determine the effect of the notification and provide the necessary support resources such as victim advocacy,, personal clergy, friends, etc.
 - (c) Officers or other department representatives should attempt to provide necessary support services for the next of kin or relatives of deceased, seriously injured, or seriously ill persons, whenever and as often as possible.

314.12 COMPLAINTS OF VICTIM'S RIGHTS VIOLATIONS

Complaints alleging a violation of a victim's rights shall be addressed in the manner described in the Personnel Complaints Policy. Investigative findings related to the complaint shall be provided to the appropriate Victim Rights Committee when required (Utah Code 63M-7-1003).

Hate Crimes

315.1 PURPOSE AND SCOPE

This department recognizes and places a high priority on any individual's constitutional right to the lawful expression of free speech or other recognized rights secured by the Constitution or laws of the state or by the Constitution or laws of the United States. When such rights are infringed upon by violence, threats or other harassment, this department will utilize all available resources to see that justice is served under the law. This policy has been developed to provide members of the Department with guidelines for identifying and investigating incidents and crimes that may be motivated by hatred or other bias.

315.1.1 FEDERAL JURISDICTION

The federal government also has the power to investigate and prosecute bias-motivated violence by providing the U.S. Department of Justice with jurisdiction over crimes of violence where the perpetrator has selected the victim because of the person's actual or perceived race, color, religion, national origin, ethnicity, gender, sexual orientation, gender identity or expression, or disability (18 USC § 249).

315.2 DEFINITIONS

Intimidate or terrorize - Means an act which causes the person to fear for his/her physical safety or damages the property of that person or another. The act must be accompanied with the intent to cause or has the effect of causing a person to reasonably fear to freely exercise or enjoy any right secured by the Constitution or laws of the state or by the Constitution or laws of the United States (Utah Code 76-3-203.3(3)).

315.3 CRIMINAL STATUTES

Utah Code 76-3-203.3 (Penalty for Hate Crimes) and Utah Code 76-3-203.4 (Hate Crimes - Aggravating Factors).

315.4 PREVENTING AND PREPARING FOR LIKELY HATE CRIMES

While it is recognized that not all crime can be prevented, this department is committed to taking a proactive approach to preventing and preparing for likely hate crimes by, among other things:

- (a) Officers should make an affirmative effort to establish contact with persons and groups within the community who are likely targets of hate crimes to form and cooperate with prevention and response networks.
- (b) Providing victim assistance and follow-up as outlined below, including community follow-up.

315.5 PROCEDURE FOR INVESTIGATING HATE CRIMES

Whenever any member of the Department receives a report of a suspected hate crime or other activity that reasonably appears to involve a potential hate crime, the following should occur:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Hate Crimes

- (a) Officers will be promptly assigned to contact the victim, witness, or reporting party to investigate the matter further as circumstances may dictate.
- (b) A supervisor should be notified of the circumstances as soon as practical.
- (c) Once “in progress” aspects of any such situation have been stabilized (e.g., treatment of victims, apprehension of present suspects), the assigned officers will take all reasonable steps to preserve available evidence that may tend to establish that a hate crime was involved.
- (d) The assigned officers will interview available witnesses, victims and others to determine what circumstances, if any, indicate that the situation may involve a hate crime.
- (e) Depending on the situation, the assigned officers or supervisor may request additional assistance from detectives or other resources to further the investigation.
- (f) The assigned officers will include all available evidence indicating the likelihood of a hate crime in the relevant reports. All related reports will be clearly marked as “Hate Crimes” and, absent prior approval of a supervisor, will be completed and submitted by the assigned officers before the end of the shift.
- (g) The assigned officers will provide the victims of any suspected hate crime with a brochure on hate crimes. Such brochures will also be available to members of the general public upon request. The assigned officers should also make reasonable efforts to assist the victims by providing available information on local assistance programs and organizations.
- (h) The assigned officers and supervisor should take reasonable steps to ensure that any such situation does not escalate further (e.g., possible Temporary Restraining Order through the District Attorney or City Attorney).

315.5.1 INVESTIGATIONS DIVISION RESPONSIBILITY

If a case is assigned to the Investigations Division, the assigned detective will be responsible for following up on the reported hate crime as follows:

- (a) Coordinate further investigation with the District Attorney and other appropriate law enforcement agencies, as appropriate.
- (b) Maintain contact with the victims and other involved individuals as needed.
- (c) Maintain statistical data on suspected hate crimes and tracking as indicated and report such data to the county or state upon request.

315.6 TRAINING

All members of the Department will receive training approved by Utah Police Officer Standards and Training on hate crime recognition and investigation.

Public Alerts

316.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for alerting the public to important information and soliciting public aid when appropriate.

316.2 POLICY

Public alerts may be employed using the Emergency Alert System (EAS), local radio, television and press organizations and other groups to notify the public of incidents, or enlist the aid of the public when the exchange of information may enhance the safety of the community. Various types of alerts may be available based upon each situation and the alert system's individual criteria.

316.3 RESPONSIBILITIES

316.3.1 MEMBER RESPONSIBILITIES

Members of the South Salt Lake Police Department should notify their supervisor, Watch Commander, or Investigations Division Supervisor as soon as practicable upon learning of a situation where public notification, a warning, or enlisting the help of the media and public could assist in locating a missing person, apprehending a dangerous person, or gathering information.

316.3.2 SUPERVISOR RESPONSIBILITIES

A supervisor apprised of the need for a public alert is responsible to make the appropriate notifications based upon the circumstances of each situation. The supervisor shall promptly notify the Chief of Police, the appropriate Division Commander and the Public Information Officer when any public alert is generated.

The supervisor in charge of the investigation to which the alert relates is responsible for the following:

- (a) Updating alerts
- (b) Canceling alerts
- (c) Ensuring all appropriate reports are completed
- (d) Preparing an after-action evaluation of the investigation to be forwarded to the Division Commander

316.4 AMBER ALERTS

AMBER Alert is the recruitment of public assistance to locate an abducted child via a widespread media alert. Utilizing the assistance of local radio, television, and press affiliates the public will be notified of the circumstances of a child's abduction and how they can assist law enforcement in the child's recovery. The goal of the AMBER Alert program is the safe return of an abducted child by establishing an effective partnership between the community, the media, and law enforcement. The AMBER Alert Plan is tested every year in January and August.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Public Alerts

The AMBER Alert does not preclude any law enforcement agency from utilizing or implementing in-house procedures, policies, or practices.

316.4.1 CRITERIA

AMBER Alerts are not to be used for cases involving custodial disputes or runaways that do not meet the criteria (Utah Code 53-10-1002). The [Department/Office] may consider issuing an Endangered Missing Advisory to inform law enforcement and the public about cases that don't meet the criteria for an AMBER Alert.

The four criteria required for an AMBER Alert are as follows (Utah Code 53-10-1002):

- (a) A confirmed abduction (non-family, non-custodial).
- (b) The child is 17-years of age or younger.
- (c) There is reason to believe the child is in imminent danger of serious bodily injury or death.
- (d) There is sufficient information available to give out to the public that could assist in the safe recovery of the victim and/or the apprehension of a suspect.

316.4.2 PROCEDURE

- (a) When the required criteria are met, the assigned officer should request that Dispatch initiate an AMBER Alert by entering the required information into the appropriate Utah Criminal Justice Information System (UCJIS) transaction.
- (b) The supervisor may also consider the following resources as the circumstances dictate:
 - 1. The regional Child Abduction Response Team (CART).
 - 2. The State of Utah CART.
 - 3. Federal Bureau of Investigation (FBI local office).
 - 4. Prompt entry of information into the Bureau of Criminal Identification (BCI) and the Department of Justice Missing Person System (NCIC).
 - 5. National Center for Missing and Exploited Children.

316.4.3 CANCELING THE AMBER ALERT

- (a) The Chief of Police or his/her designee will make the determination when to cancel an AMBER alert.
 - 1. Once the alert has been canceled, Dispatch must cancel the alert by using the UCJIS Utah Amber Alert (UAA) transaction.
 - 2. A "NLETS AM" message will be sent to surrounding states notifying them of the cancellation.
- (b) The following fields are required when canceling an AMBER Alert:
 - 1. ORI, type, agency, phone, and authorizing administrator.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Public Alerts

2. Victim name.
 3. Victim date of birth.
- (c) Contact will then be made with the BCI Telecommunications at (801) 965-4446 to verify they received the AMBER Alert cancellation notice via UCJIS.

316.5 BLUE ALERTS

The BLUE alert means information sent through State of Utah Bureau of Criminal Identification relating to a serious injury or death of a law enforcement officer in the line of duty or an officer who is missing in connection with the officer's official duties or an imminent and credible threat that an individual intends to cause the serious injury or death of a law enforcement officer. UCJIS Help Desk (801) 965-4446.

316.5.1 CRITERIA

The four criteria required for a BLUE Alert are as follows:

- (a) A law enforcement officer has been killed, seriously injured or assaulted with a deadly weapon by the suspect.
- (b) The suspect is an imminent threat to the public and other law enforcement personnel.
- (c) There is information available for the public about the suspect, the suspect's vehicle and vehicle tag.
- (d) Public dissemination of available information will help avert further harm or accelerate apprehension of the suspect.

316.5.2 PROCEDURE

BLUE Alerts are initiated solely by Utah law enforcement agencies through UCJIS and by contacting the BCI.

In the event of an assault with a deadly weapon, serious bodily injury or death of an officer, the following procedures designed to alert the media shall be followed.

- (a) The Public Information Officer, Watch Commander or Detective Supervisor will prepare an initial press release that includes all available information which might aid in locating the suspect:
 1. The license number and/or any other available description or photograph of the vehicle
 2. Photograph, description and/or identification of the suspect
 3. The suspect's identity, age and description, if known
 4. Detail regarding location of incident, direction of travel, potential destinations, if known
 5. Name and phone number of the Public Information Officer or other authorized individual to handle media liaison
 6. A telephone number for the public to call in with leads/information

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Public Alerts

- (b) The press release should be sent to the local television and radio stations.
- (c) The information in the press release should also be forwarded to the local emergency communications center so that general broadcasts can be made to local law enforcement agencies.

316.6 ENDANGERED MISSING ADVISORY

The Endangered Missing Advisory is a system to rapidly disseminate information about a missing and/or endangered person to law enforcement agencies and the media. The Endangered Missing Advisory is a voluntary partnership between law enforcement and local broadcasters for notifying the public about a missing and endangered person. The advisories are initiated solely by Utah law enforcement agencies.

316.6.1 CRITERIA

The following criteria must be met to initiate an Endangered Missing Advisory:

- (a) The person must be missing under unexplained or suspicious circumstances.
- (b) The person is believed to be in danger because of age, health, mental or physical disability, environment or weather conditions, in the company of a potentially dangerous person or some other factor that may put the person in peril.
- (c) There is information that could assist the public in the safe recovery of the missing person.

316.6.2 PROCEDURE

When the required criteria are met, the assigned officer should request that Dispatch activate an Endangered Missing Advisory by entering descriptive information and officer contact information into the appropriate UCJIS transaction and by contacting the Bureau of Criminal Identification. The assigned officer is responsible to ensure that information is entered into the National Crime Information Center (NCIC) database.

316.7 SILVER ALERTS

Silver Alerts are used to provide a statewide system for the rapid dissemination of information regarding a missing endangered adult (Utah Code 53-10-702).

316.7.1 CRITERIA

The following criteria must be met to initiate a Silver Alert:

- (a) The person is reported missing.
- (b) The person reported missing is 60 years of age or older or has some form of Alzheimer's disease or other forms of dementia resulting in continual loss of memory or awareness dementia (Utah Code 53-10-703).

316.7.2 PROCEDURE

When the required criteria are met, the assigned officer shall request that Dispatch initiate a Silver Alert by contacting BCI through the UCJIS system and providing descriptive information,

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Public Alerts

the specific area in which the missing person was last seen, and the officer contact information (UT ADC R722-400-4).

Adult Abuse

317.1 PURPOSE AND SCOPE

The purpose of this policy is to provide members of the Department with direction and understanding of their role in the prevention, detection and intervention in incidents of elder abuse. It is the policy of the South Salt Lake Police Department to treat reports of violence against elderly persons as high priority criminal activity that is to be fully investigated regardless of the relationship between the victim and the suspect(s).

317.2 DEFINITIONS

For purposes of this policy, the following definitions are provided (Utah Code 76-5-111).

Abandonment - Any knowing or intentional action or inaction, including desertion, by a person or entity acting as a caretaker for a vulnerable adult that leaves the vulnerable adult without the means or ability to obtain necessary food, clothing, shelter or medical or other health care (Utah Code 76-5-111(1)(a)).

Abuse - Attempting to cause harm, intentionally or knowingly causing harm or intentionally or knowingly placing another in fear of imminent harm and includes (Utah Code 76-5-111(1)(b)):

- Unreasonable or inappropriate use of physical restraint, medication or isolation that causes or is likely to cause harm to a vulnerable adult, which is in conflict with a physician's orders or used as an unauthorized substitute for treatment, unless that conduct furthers the health and safety of the adult.
- Emotional or psychological abuse.
- Sexual offense as described in Utah Code 76-5-101 et seq.
- Deprivation of life sustaining treatment, except as provided in Utah Code 75-2a-101 et seq., or when informed consent, as defined in Utah Code 76-5-111, has been obtained.

Caretaker - Any person, entity, corporation or public institution that assumes the responsibility of providing a vulnerable adult with care, food, shelter, clothing, supervision, medical or other health care or other necessities. Caretaker includes a relative by blood or marriage, a household member, a person who is employed or who provides volunteer work, or a person who contracts or is under court order to provide care (Utah Code 76-5-111(1)(d)).

Elder abuse - Abuse, neglect or exploitation of an elder adult (Utah Code 76-5-111(1)(b)). An adult is not considered abused, neglected or a vulnerable adult for the reason that the adult has chosen to rely solely upon religious, non-medical forms of healing in lieu of medical care.

Elder adult - Any person 65-years of age or older (Utah Code 76-5-111(1)(f)).

Emotional or psychological abuse - Intentional or knowing verbal or nonverbal conduct directed at a vulnerable adult, including ridiculing, intimidating, yelling, swearing, threatening, isolating, coercing, harassing or other forms of intimidating behavior that result or could result in the

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Adult Abuse

vulnerable adult suffering mental anguish or emotional distress, including fear, humiliation, degradation, agitation, confusion or isolation (Utah Code 76-5-111(1)(i)).

Exploitation - A person commits the offense of exploitation of a vulnerable adult when the person:

- Is in a position of trust and confidence or has a business relationship with the vulnerable adult and knowingly, by deception or intimidation, obtains or uses or endeavors to obtain or use, the vulnerable adult's funds, credit, assets or property with the intent to temporarily or permanently deprive the vulnerable adult of the use, benefit or possession of his/her property for the benefit of someone other than the vulnerable adult.
- Knows or should know that the vulnerable adult lacks the capacity to consent, and obtains or uses, or endeavors to obtain or use, or assists another in obtaining or using or endeavoring to obtain or use, the vulnerable adult's funds, assets or property with the intent to temporarily or permanently deprive the vulnerable adult of the use, benefit or possession of his/her property for the benefit of someone other than the vulnerable adult.
- Unjustly or improperly uses or manages the resources of a vulnerable adult for the profit or advantage of someone other than the vulnerable adult.
- Unjustly or improperly uses a vulnerable adult's power of attorney or guardianship for the profit or advantage of someone other than the vulnerable adult.
- Involves a vulnerable adult who lacks the capacity to consent in the facilitation or furtherance of any criminal activity.
- Commits sexual exploitation of a vulnerable adult (Utah Code 76-5-111(4)).

Harm - Pain, mental anguish, emotional distress, hurt, physical or psychological damage, physical injury, serious physical injury, suffering or distress inflicted knowingly or intentionally (Utah Code 76-5-111(1)(i)).

Neglect - Any of the following:

- Failure of a caretaker to provide nutrition, clothing, shelter, supervision, personal care or dental, medical or other health care.
- Failure to provide protection from health and safety hazards or maltreatment.
- Failure of a caretaker to provide care to a vulnerable adult in a timely manner and with the degree of care that a reasonable person in a like position would exercise.
- A pattern of conduct by a caretaker without the vulnerable adult's informed consent, resulting in deprivation of food, water, medication, health care, shelter, cooling, heating or other services necessary to maintain the vulnerable adult's well-being.
- Knowing or intentional failure by a caretaker to carry out a prescribed treatment plan that causes or is likely to cause harm to the vulnerable adult.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Adult Abuse

- Self-neglect by the vulnerable adult (Utah Code 76-5-111(1)(i-v).
- Abandonment by a caretaker (Utah Code 76-5-111(1)(a)).

Vulnerable adult - An elder adult, or an adult who has a mental or physical impairment which substantially affects that person's ability to:

- Provide personal protection.
- Provide necessities, such as food, shelter, clothing or mental or other health care.
- Obtain services necessary for health, safety or welfare.
- Carry out the activities of daily living.
- Manage the adult's own resources.
- Comprehend the nature and consequences of remaining in a situation of abuse, neglect or exploitation (Utah Code 76-5-111(1)(t)).

317.3 MANDATORY NOTIFICATION

Members of the South Salt Lake Police Department shall notify Adult Protective Services (APS) when the member has reason to believe that an elder or vulnerable adult has been abused.

For purposes of notification (Utah Code 26B-6-201):

- (a) Abuse includes but is not limited to the intentional infliction of harm or emotional abuse, the exploitation, or the neglect of an elder or vulnerable adult.
- (b) Elder adult means someone age 65 or older.
- (c) Vulnerable adult means an elder adult or a dependent adult age 18 or older who has a mental or physical impairment that substantially affects the person's ability to provide for themselves or their own personal protection.

317.3.1 NOTIFICATION PROCEDURE

Notification should occur either by telephone or by utilizing the online reporting form provided by APS immediately or as soon as practicable.

317.4 ELDER ABUSE REPORTING

Every allegation of elder abuse shall be documented. When documenting vulnerable adult abuse cases, the following information should be included in the report:

- Current location of the victim
- Victim's condition/nature and extent of injuries, neglect or loss
- Names of agencies and personnel requested and who are on-scene

Reporting cases of vulnerable adult abuse is confidential and will only be released in accordance with the Release of Records and Information Policy.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Adult Abuse

Officers investigating the abuse of a vulnerable adult shall complete all appropriate Department and state forms.

317.5 INVESTIGATIONS AND REPORTING

All reported or suspected cases of adult abuse require investigation and a report, even if the allegations appear unfounded or unsubstantiated.

Investigations and reports related to suspected cases of adult abuse should address, as applicable:

- (a) The overall basis for the contact. This should be done by the investigating officer in all circumstances where a suspected adult abuse victim is contacted.
- (b) Any relevant statements the victim may have made and to whom the victim made the statements.
- (c) If a person is taken into protective custody, the reasons, the name and title of the person making the decision, and why other alternatives were not appropriate.
- (d) Documentation of any visible injuries or any injuries identified by the victim. This should include photographs of such injuries, if practicable.
- (e) Whether the victim was transported for medical treatment or a medical examination.
- (f) Whether the victim identified a household member as the alleged perpetrator, and a list of the names of any other potential victims or witnesses who may reside in the residence.
- (g) Identification of any prior related reports or allegations of abuse, including other jurisdictions, as reasonably known.
- (h) Previous addresses of the victim and suspect.
- (i) Other potential witnesses who have not yet been interviewed, such as relatives or others close to the victim's environment.
- (j) If any photographs or audio and/or video recordings of the victim were taken (Utah Code 26B-6-206).

Any unexplained death of an adult who was in the care of a guardian or caretaker should be considered as potential adult abuse and investigated similarly.

317.6 PROTECTIVE CUSTODY

Before taking an adult abuse victim into protective custody when facts indicate the adult may not be able to care for him/herself, the officer should make reasonable attempts to contact APS. Generally, removal of an adult abuse victim from his/her family, guardian or other responsible adult should be left to the welfare authorities when they are present or have become involved in an investigation.

Generally, members of this department should remove an adult abuse victim from his/her family or guardian without a court order only when no other effective alternative is reasonably available and immediate action reasonably appears necessary to protect the victim. Prior to taking an adult

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Adult Abuse

abuse victim into protective custody, the officer should take reasonable steps to deliver the adult to another qualified legal guardian, unless it reasonably appears that the release would endanger the victim or result in abduction. If this is not a reasonable option, the officer shall ensure that the adult is delivered to APS.

Whenever practicable, the officer should inform a supervisor of the circumstances prior to taking an adult abuse victim into protective custody. If prior notification is not practicable, officers should contact a supervisor promptly after taking the adult into protective custody.

When adult abuse victims are under state control, have a state-appointed guardian or there are other legal holdings for guardianship, it may be necessary or reasonable to seek a court order on behalf of the adult victim to either remove the adult from a dangerous environment (protective custody) or restrain a person from contact with the adult.

317.6.1 REMOVAL AND TRANSPORT OF ADULT ABUSE VICTIM

Removal and transport of an adult abuse victim by an officer may only occur under the following conditions (Utah Code 26B-6-207):

- (a) The officer has probable cause to believe that the adult abuse victim will suffer serious physical injury if not immediately removed and transported to a safe environment.
- (b) The adult abuse victim either refuses to consent or lacks capacity to consent to the removal and transport.
- (c) There is not time to notify interested parties or to secure a warrant or other court order for the removal and transport.
- (d) The person will be taken to a medical or shelter facility.

The officer removing and transporting an adult abuse victim shall notify APS within four hours to request that an emergency protective order be obtained from the court (Utah Code 26B-6-207).

317.7 QUALIFIED INVESTIGATORS

Qualified investigators should be available to investigate cases of adult abuse. These investigators should:

- (a) Conduct interviews in appropriate interview facilities.
- (b) Be familiar with forensic interview techniques specific to adult abuse investigations.
- (c) Present all cases of alleged adult abuse to the prosecutor for review.
- (d) Coordinate with other enforcement agencies, social service agencies and facility administrators as needed.
- (e) Provide referrals to therapy services, victim advocates, guardians and support for the victim and family as appropriate.
- (f) Participate in or coordinate with multidisciplinary investigative teams as applicable.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Adult Abuse

317.7.1 MANDATORY COORDINATION

Members shall coordinate with APS to provide protection to victims and to investigate cases of elder or vulnerable adult abuse (Utah Code 26B-6-205).

317.8 INTERVIEWS

317.8.1 PRELIMINARY INTERVIEWS

Absent extenuating circumstances or impracticality, officers should audio record the preliminary interview with a suspected adult abuse victim. Officers should avoid multiple interviews with the victim and should attempt to gather only the information necessary to begin an investigation. When practicable, investigating officers should defer interviews until a person who is specially trained in such interviews is available.

317.8.2 DETAINING VICTIMS FOR INTERVIEWS

An officer should not detain an adult involuntarily who is suspected of being a victim of abuse solely for the purpose of an interview or physical exam without his/her consent or the consent of a guardian unless one of the following applies:

- (a) Exigent circumstances exist, such as:
 - 1. A reasonable belief that medical issues of the adult need to be addressed immediately.
 - 2. A reasonable belief that the adult is or will be in danger of harm if the interview or physical exam is not immediately completed.
 - 3. The alleged offender is a family member or guardian and there is reason to believe the adult may be in continued danger.
- (b) A court order or warrant has been issued.

317.9 MEDICAL EXAMINATIONS

When an adult abuse investigation requires a medical examination, the investigating officer should obtain consent for such examination from the victim, guardian, agency or entity having legal custody of the adult. The officer should also arrange for the adult's transportation to the appropriate medical facility.

In cases where the alleged offender is a family member, guardian, agency or entity having legal custody and is refusing to give consent for the medical examination, officers should notify a supervisor before proceeding. If exigent circumstances do not exist or if state law does not provide for officers to take the adult for a medical examination, the supervisor should consider other government agencies or services that may obtain a court order for such an examination.

317.10 DRUG-ENDANGERED VICTIMS

A coordinated response by law enforcement and social services agencies is appropriate to meet the immediate and longer-term medical and safety needs of an adult abuse victim who has been exposed to the manufacturing, trafficking or use of narcotics.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Adult Abuse

317.10.1 SUPERVISOR RESPONSIBILITIES

The Investigations Division supervisor should:

- (a) Work with professionals from the appropriate agencies, including APS, other law enforcement agencies, medical service providers and local prosecutors, to develop community-specific procedures for responding to situations where there are adult abuse victims endangered by exposure to methamphetamine labs or the manufacture and trafficking of other drugs.
- (b) Activate any available interagency response when an officer notifies the Investigations Division supervisor that he/she has responded to a drug lab or other narcotics crime scene where an adult abuse victim is present or where evidence indicates that an adult abuse victim lives.
- (c) Develop a report format or checklist for use when officers respond to drug labs or other narcotics crime scenes. The checklist will help officers document the environmental, medical, social and other conditions that may affect the adult.

317.10.2 OFFICER RESPONSIBILITIES

Officers responding to a drug lab or other narcotics crime scene where an adult abuse victim is present or where there is evidence that an adult abuse victim lives should:

- (a) Document the environmental, medical, social and other conditions of the adult, using photography as appropriate and the checklist or form developed for this purpose.
- (b) Notify the Investigations Division supervisor so an interagency response can begin.

317.11 STATE MANDATES AND OTHER RELEVANT LAWS

Utah requires or permits the following:

317.11.1 RECORDS SECTION RESPONSIBILITIES

The Records Section is responsible for:

- (a) Providing a copy of the adult abuse report to APS as required by law.
- (b) Retaining the original adult abuse report with the initial case file.

317.11.2 RELEASE OF REPORTS

Information related to incidents of adult abuse or suspected adult abuse shall be confidential and may only be disclosed pursuant to state law and the Records Maintenance and Release Policy (Utah Code 26B-6-212).

317.11.3 NOTIFICATION UPON ARREST OR ISSUANCE OF A CITATION

When an officer arrests or issues a citation to a person 18 years of age or older for adult abuse, the officer shall provide the person with the written notice required by Utah Code 78B-7-802. Victims shall be provided notice in accordance with the Victim and Witness Assistance Policy.

317.12 TRAINING

The Department should provide training on best practices in adult abuse investigations to members tasked with investigating these cases. The training should include:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Adult Abuse

- (a) Participating in multidisciplinary investigations, as appropriate.
- (b) Conducting interviews.
- (c) Availability of therapy services for adults and families.
- (d) Availability of specialized forensic medical exams.
- (e) Cultural competence (including interpretive services) related to adult abuse investigations.
- (f) Availability of victim advocates or other support.

Missing Persons

318.1 PURPOSE AND SCOPE

This policy provides guidance for handling missing person investigations.

318.1.1 DEFINITIONS

Definitions related to this policy include:

At risk - Includes persons who:

- (a) Are 13 years of age or younger.
- (b) Regardless of age, are believed or determined to be experiencing one or more of the following circumstances:
 - 1. Out of the zone of safety for their chronological age and developmental stage
 - 2. Mentally or behaviorally disabled
 - 3. Drug dependent, including prescribed medication and/or illegal substances, and the dependency is potentially life-threatening
 - 4. Absent from home for more than 24 hours before being reported to law enforcement as missing
 - 5. In a life-threatening situation
 - 6. In the company of others who could endanger their welfare
 - 7. Absent in a way that is inconsistent with established patterns of behavior and cannot be readily explained. Most children have an established and reasonably predictable routine.
 - 8. Involved in a situation that would cause a reasonable person to conclude the person should be considered at risk

Missing person - Any person who is reported missing to law enforcement when that person's location is unknown. This includes a person who is missing from the person's home environment and is physically or mentally disabled, missing under circumstances that indicate that the person is endangered, missing involuntarily, or a victim of a catastrophe (Utah Code 26B-8-130).

Missing person networks - Databases or computer networks that are available to law enforcement and are suitable for obtaining information related to missing person investigations. This includes the National Crime Information Center (NCIC), the National Missing and Unidentified Persons System (NamUs), and the Utah Bureau of Criminal Identification (BCI) Missing Persons Clearinghouse.

318.2 POLICY

The South Salt Lake Police Department does not consider any report of a missing person to be routine and assumes that the missing person is in need of immediate assistance until an investigation reveals otherwise. Priority shall be given to missing person cases over property-

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Missing Persons

related cases. Members will initiate an investigation into all reports of missing persons, regardless of the length of time the person has been missing.

318.2.1 RESPONSIBILITIES OF THE PRIMARY ASSIGNED OFFICER

The officer assigned as the primary responder to the incident should prioritize and perform the following tasks:

- (a) Unless acting in direct response to the child's safety, respond directly and promptly to the individual who made the initial report.
- (b) Conduct interviews with the parents or other person who made the initial report in order to gain insight into the circumstances surrounding the disappearance and gather other information needed to conduct an initial assessment of the case.
- (c) Obtain a detailed description of the missing child, several recent photographs, and any recent videotapes as available and forward with the report. Photos should immediately be copied and provided for neighborhood canvas and search teams.
- (d) Regardless of any search that may have been conducted previously by parents or others, verify that the child is missing by conducting a consensual search of the house and grounds to include places where a child could be hiding, trapped, or asleep.
- (e) Confirm the child's custody status, whether a custody dispute or similar problem exists between the parents, whether a restraining order is in effect, or whether the child has expressed an interest in living with the non-custodial parent.
- (f) Determine when, where, and by whom the child was last seen.
- (g) Interview those who last saw the child.
- (h) Secure and safeguard the incident scene and/or place last seen as a potential crime scene.
- (i) Ensure that personnel do not tamper with potential evidence
- (j) Contact a supervisor to have a Crime Scene Technician respond to examine the scene.
- (k) Identify any areas of the incident scene or the home that have been disrupted since the child's disappearance.
 - 1. In particular, the child's bedroom, bed clothing, and related areas and items should be secured and protected until evidence and identification material such as hair, fingerprints, or bite marks can be collected by Crime Scene Technicians.
- (l) Identify the Zone of Safety for the child's age and developmental stage.
- (m) Based on available information, make an initial determination of the type of case, the need for additional resources, and whether the incident should be initially classified as "Unusual Circumstances" as defined in this policy.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Missing Persons

- (n) If the child was abducted, obtain a description of the abductors if available, the mode of travel, vehicle description, and related information.
- (o) This information should be given to police dispatch as soon as it is obtained.
- (p) If the abductor is a family member, obtain photographs of the suspect.
- (q) Contact a supervisor to begin steps to initiate an Attempt to Locate (ATL), Reverse 911, A Child is Missing Alert, Endangered Person Advisory, AMBER Alert, and Utah Statewide CART.
- (r) Canvas the neighborhood, as soon as possible, to identify and interview residents and others within the area the child was abducted. Identify all vehicles parked within the neighborhood. Keep detailed logs of all information gathered.
- (s) Fully identify and separately interview anyone at the scene of the disappearance.
- (t) Even if the child's disappearance occurred elsewhere, a thorough home search should be conducted. Obtain written permission to conduct the search and, with the assistance of additional personnel, search the residence, out building(s) and other structures, vehicles (including trunk), and related property.
- (u) Prepare a chronological account of actions taken and information obtained from point of contact to relief.

318.2.2 RESPONSIBILITIES OF SUPERVISOR(S) ON DUTY

- (a) Obtain a briefing from the primary responder and other agency personnel at the scene sufficient to determine the scope and complexity of the case and develop an appropriate response. Conduct the briefing away from family, friends, and other involved individuals.
- (b) Ensure that primary responder responsibilities, as outlined in the foregoing section, have been fully and properly carried out.
- (c) Determine if additional personnel and resources are needed to assist in the investigation. If so, contact the Division Commanders and make call-outs accordingly.
- (d) If necessary, establish a command post to assist in field management of the search and the investigation.
- (e) Appoint a search operations coordinator to organize and coordinate search efforts.
- (f) Contact the Public Information Officer to deal with media inquiries.
- (g) Ensure that all required notifications have been made, and other local law enforcement agencies have been notified of pertinent information.
- (h) Establish a liaison with the family who can explain police efforts and work with the family to uncover any information useful to the investigation.
- (i) Notify the Detective Sergeant of all information known at the time and request a Crime Scene Technician and a Investigation(s).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Missing Persons

- (j) Determine the need to initiate an Attempt to Locate (ATL), Reverse 911, A Child is Missing Alert, Endangered Person Advisory, AMBER Alert, and Utah Statewide CART.
- (k) Ensure notifications to the Office of the Chief of Police and Division Commander.
- (l) Determine the correct NCIC Missing Person File category (disability, endangered, involuntary, juvenile, or catastrophe) then request that VECC or other authorized personnel promptly enter this into NCIC.
- (m) If the missing person is under the age of 21, the NCIC entry will be entered within two hours of receipt of the report.

318.2.3 RESPONSIBILITIES OF THE ASSIGNED DETECTIVE

- (a) Obtain a briefing from agency personnel at the scene.
- (b) Verify the accuracy of all descriptive information concerning the child, being alert to facts or statements that may conflict with those obtained by the primary responder or supervisor.
- (c) Obtain a general history of recent family dynamics from family members, neighbors, classmates, teachers, school counselors, and other persons who may have had close personal interaction with the child and/or family.
- (d) Conduct in-depth fact-finding interviews with all witnesses, friends or relatives of the missing child, teachers, classmates, or others who knew and/or routinely interacted with the child, placing particular emphasis on identifying and conflicting information offered by these or other individuals.
- (e) Review any records generated about the family or child from the police agency, social service agencies, schools, and related organizations or agencies.
- (f) Reassess the need for additional resources and specialized services to include Utah Statewide Child Abduction Response Team (CART), specialized search and rescue operations, Utah's Missing Children's Clearinghouse, and federal agencies such as the FBI and the National Center for Missing and Exploited Children.
- (g) If the case is not resolved promptly, update descriptive records and those entered into state and federal missing persons databases to include dental characteristics, scars, marks, tattoos, fingerprints, and additional articles of clothing, jewelry, or possessions not previously itemized.
- (h) Determine whether a computer voice stress analyzer examination or polygraph is warranted and request such an examination where indicated; parents, guardians, or other persons as appropriate.
- (i) Monitor media relations to include review of all agency releases to the media to ensure that information is not released that will compromise the investigation.
- (j) Provide the family with whatever support is possible and appropriate. Provide them with a copy of the Family Survival Guide prepared by the Office of Juvenile Justice

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Missing Persons

and Delinquency Prevention or contact the National Center for Missing and Exploited Children to have one sent to them via overnight mail.

318.2.4 RUNAWAY JUVENILES

- (a) The officer taking the complaint will ensure all available information requested on the Runaway Report form has been obtained. The officer will then submit a report narrative that is based upon the interview of the complainant, using the same professional investigative skills expected on any reported incident.
 - 1. If there are immediate leads that can be followed up on, the officer will attempt to locate the runaway.
 - 2. Enter the runaway on NCIC.
 - 3. If a patrol officer locates the runaway, it will be the officer's responsibility to have the runaway removed from NCIC and conduct a follow up interview. The interview will cover the following, including but not limited to:
 - (a) Why the child ran away.
 - (b) What the child did while gone.
 - (c) Who the child associated with, including names and addresses.
- (b) The Records Division has responsibility for the report after the officer has turned it in.
 - (a) The Records Division will enter the Runaway Report into the Records Management System and maintain the Runaway report form in the filing system.
 - (b) All Runaway Reports will be referred to investigators electronically.
 - (c) If the runaway was recovered by the Patrol Division, the report will still be referred to the Investigations for a follow up interview.
- (c) The investigations Secretary will be responsible for assigning Runaway Reports to Investigations for follow-up. The Detective Sergeant will be responsible for reviewing Runway Reports.
- (d) The assigned investigator will be responsible for making contact with the complainant within three workdays of receiving the report.
 - (a) Any leads will be followed up, and the investigator will keep in contact with the complainant at least once a week.
 - (b) Supplemental reports will be written to reflect contacts and progress.
 - (c) If the child is located while the case is assigned to the investigator, an interview of the child will be performed by the recovering officer or the assigned investigator. The interview will cover the following, including but not limited to:
 - (a) Why the child ran away.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Missing Persons

- (b) What the child did while gone.
 - (c) Who the child associated with, including names and addresses.
- (e) If the investigator determines the reason for the runaway was because of victimization or criminal activity, the information will be followed up by the investigator.
 - 1. The investigator will be responsible to ensure the runaway is removed from NCIC.
- (f) Should the runaway not be located after thirty days, a BCI packet will be filled out and submitted.
 - 1. Also a poster will be made for distribution to other agencies through SIAC and/or Utah Missing Person Clearinghouse.
- (g) Upon request from the Utah Missing Person Clearinghouse for follow up, the assigned detective will fill out and return the supplemental information packet.
- (h) Once the juvenile is located all above listed interviews and investigations will be completed.

318.3 REQUIRED FORMS AND BIOLOGICAL SAMPLE COLLECTION KITS

The Investigations Division supervisor shall ensure the following forms and kits are developed and available:

- Missing person report form
- Missing person investigation checklist that provides investigation guidelines and resources that could be helpful in the early hours of a missing person investigation
- Missing person school notification form
- Medical records release form
- Biological sample collection kits

318.4 ACCEPTANCE OF REPORTS

Any member encountering a person who wishes to report a missing person or runaway shall render assistance without delay. This can be accomplished by accepting the report via telephone or in-person and initiating the investigation. Those members who do not take such reports or who are unable to give immediate assistance shall promptly dispatch or alert a member who can take the report.

A report shall be accepted in all cases and regardless of where the person was last seen, where the person resides or any question of jurisdiction.

318.5 INITIAL INVESTIGATION

Officers or other members conducting the initial investigation of a missing person should take the following investigative actions, as applicable:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Missing Persons

- (a) Respond to a dispatched call as soon as practicable.
- (b) Interview the reporting party and any witnesses to determine whether the person qualifies as a missing person and, if so, whether the person may be at risk.
- (c) Notify a supervisor immediately if there is evidence that a missing person is either at risk or may qualify for a public alert, or both (see the Public Alerts Policy).
- (d) Broadcast a "Be on the Look-Out (BOLO) bulletin" if the person is under 16 years of age or there is evidence that the missing person is at risk. The BOLO should be broadcast as soon as practicable but in no event more than one hour after determining the missing person is under 16 years of age or may be at risk.
- (e) Ensure that entries are made into the appropriate missing person networks:
 - 1. Immediately, when the missing person is at risk.
 - 2. In all other cases, as soon as practicable, but not later than two hours from the time of the initial report (34 USC § 41308).
- (f) Complete the appropriate report forms accurately and completely and initiate a search as applicable according to the facts.
- (g) Collect and/or review:
 - 1. A photograph and fingerprint card of the missing person, if available.
 - 2. A voluntarily provided biological sample of the missing person, if available (e.g., toothbrush, hairbrush).
 - 3. Any documents that may assist in the investigation, such as court orders regarding custody.
 - 4. Any other evidence that may assist in the investigation, including personal electronic devices (e.g., cell phones, computers).
- (h) When circumstances permit and if appropriate, attempt to determine the missing person's location through their telecommunications carrier.
- (i) Contact the appropriate agency if the report relates to a missing person report previously made to another agency and that agency is actively investigating the report. When this is not practicable, the information should be documented in an appropriate report for transmission to the appropriate agency. If the information relates to an at-risk missing person, the member should notify a supervisor and proceed with reasonable steps to locate the missing person.

318.6 REPORT PROCEDURES AND ROUTING

Members should complete all missing person reports and forms promptly and advise the appropriate supervisor as soon as a missing person report is ready for review.

318.6.1 SUPERVISOR RESPONSIBILITIES

The responsibilities of the supervisor shall include, but are not limited to:

- (a) Reviewing and approving missing person reports upon receipt.
 - 1. The reports should be promptly sent to the Records Section.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Missing Persons

- (b) Ensuring resources are deployed as appropriate.
- (c) Initiating a command post as needed.
- (d) Ensuring applicable notifications and public alerts are made and documented.
- (e) Ensuring that records have been entered into the appropriate missing persons networks.
- (f) Taking reasonable steps to identify and address any jurisdictional issues to ensure cooperation among agencies.
 - 1. If the case falls within the jurisdiction of another agency, the supervisor should facilitate transfer of the case to the agency of jurisdiction.

318.6.2 RECORDS SECTION RESPONSIBILITIES

The responsibilities of the Records Section receiving member shall include, but are not limited to:

- (a) As soon as reasonable under the circumstances, notifying and forwarding a copy of the report to the agency of jurisdiction for the missing person's residence in cases where the missing person is a resident of another jurisdiction.
- (b) Notifying and forwarding a copy of the report to the agency of jurisdiction where the missing person was last seen.
- (c) Notifying and forwarding a copy of the report to the agency of jurisdiction for the missing person's intended or possible destination, if known.
- (d) Forwarding a copy of the report to the Investigations Division.
- (e) Coordinating with the NCIC Terminal Contractor for Utah to have the missing person record in the NCIC computer networks updated with additional information obtained from missing person investigations (34 USC § 41308).

318.7 INVESTIGATIONS DIVISION FOLLOW-UP

In addition to completing or continuing any actions listed above, the investigator assigned to a missing person investigation:

- (a) Should ensure that the missing person's school is notified within 10 days if the missing person is a juvenile.
 - 1. The notice shall be in writing and should also include a photograph.
 - 2. The investigator should meet with school officials as appropriate to stress the importance of including the notice in the child's student file, along with the investigator's contact information if the school receives a call requesting the transfer of the missing child's files to another school.
- (b) Should re-contact the reporting party and/or other witnesses within 30 days of the initial report and within 30 days thereafter to determine if any additional information has become available.
- (c) Should consider contacting other agencies involved in the case to determine if any additional information is available.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Missing Persons

- (d) Shall verify and update the Missing Persons Clearinghouse, NCIC and any other applicable missing person networks within 30 days of the original entry into the networks and every 30 days thereafter until the missing person is located (34 USC § 41308).
- (e) Should continue to make reasonable efforts to locate the missing person and document these efforts at least every 30 days.
- (f) Shall maintain a close liaison with state and local child welfare systems and the National Center for Missing and Exploited Children (NCMEC) if the missing person is under the age of 21 and shall promptly notify NCMEC when the person is missing from a foster care family home or childcare institution (34 USC § 41308).
- (g) Should make appropriate inquiry with the [MedicalExaminer/JOP].
- (h) Should obtain and forward medical and dental records, photos, X-rays, and biological samples, as applicable.
- (i) Shall attempt to obtain the most recent photograph for persons under 18 years of age if it has not been obtained previously and forward the photograph to the Utah BCI and enter the photograph into applicable missing person networks (34 USC § 41308).
- (j) In the case of an at-risk missing person or a person who has been missing for an extended time, should consult with a supervisor regarding seeking federal assistance from the FBI and the U.S. Marshals Service (28 USC § 566).

318.7.1 ENDANGERED MISSING ADVISORY

The Endangered Missing Advisory is a system to rapidly disseminate information about a missing and/or endangered person to law other enforcement agencies and the media. The Endangered Missing Advisory is a voluntary partnership between law enforcement and local broadcasters for notifying the public about a missing and endangered person. Advisories are initiated solely by Utah law enforcement agencies.

- (a) The handling officer must determine if the guideline for an Endangered Missing Advisory is met:
 - 1. Is the person missing under unexplained or suspicious circumstances?
 - 2. Is the person believed to be in danger because of age, health, mental or physical disability, environment or weather conditions, in the company of a potentially dangerous person or some other factor that may put the person in peril?
 - 3. Is there information that could assist the public in the safe recovery of the missing person?
 - 4. Do the circumstances fail to meet the criteria for an AMBER Alert?
 - (a) If AMBER Alert criteria are met immediately follow the protocol to issue an AMBER Alert
- (b) Endangered Missing Advisory Activation:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Missing Persons

- (a) Prepare the "Endangered Missing Advisory" by entering an "Attempt To Locate" (ATL) on the Utah Criminal Justice Information System (UCJIS). Write "Endangered Missing Advisory" in the title of the entry.
- (b) Contact the Bureau of Criminal Identification (BCI) at (801) 965-4686 / After business hours use (801) 965-4446 to verify they received the advisory via UCJIS.
- (c) The Department will enter the information into the National Crime Information Center (NCIC) database.
- (d) Send the information to the National Center for Missing and Exploited Children (NCMEC) if the person is under the age of 18. NCMEC can also be contacted via telephone at (800) THE-LOST (800-843-5678).
- (e) All Utah law enforcement agencies will be notified with a state wide "Attempt to Locate"/Endangered Missing entry.
- (f) Broadcasters and the media will then be notified by e-mail.
- (g) Freeway signs will not be activated for an Endangered Missing Advisory. The purpose for the advisory is for media notification only.

318.7.2 ACTIVATION OF UTAH STATEWIDE CHILD ABDUCTION RESPONSE TEAM (CART)

- (a) Criteria for activation of CART:
 - 1. CART will respond to all requests for assistance in locating a missing, endangered, or abducted child.
 - 2. In the case of a suspected or verified abduction, it is mandatory that CART be called out in the very early stages of the investigation.
 - 3. In the case of a missing or endangered child, the Division Commander will access the situation and determine the need for activating CART.
- (b) Activation of CART:
 - 1. Once the determination has been made to call out CART, the following procedures will take place:
 - (a) Notify the dispatch center of the need to call out CART.
 - (b) The Division Commander will notify the Chief of Police.
 - (c) The Utah Statewide CART team can also be contacted by calling the Utah Department of Public Safety, Salt Lake Communications Center at (801) 887-3800.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Missing Persons

- (d) The Utah Statewide CART has identified commanders, who will respond with the team and act as a liaison between CART and the on-scene commander.

318.7.3 UNIDENTIFIED CHILDREN

- (a) An officer/detective who is assigned to the report of an unidentified person who appears to be a child, whether living or deceased is responsible for completion of the following, including but not limited to:
 - 1. Obtain a complete description of the individual.
 - 2. Enter the child's description into the NCIC Unidentified Person File.
 - 3. Utilize available resources to identify the child, to include:
 - (a) The National Center for Missing and Exploited Children.
 - (b) Utah's Missing and Exploited Children Clearinghouse.
 - (c) Medical Examiner's Office for the State of Utah.
- (b) Once identification has been made, cancel all notifications.

318.7.4 RECOVERY AND/OR CASE CLOSURE

During the follow-up, an officer assigned to the recovery or return of a missing child shall complete the following tasks, among his/her other responsibilities.

- (a) Verify the identity of the returned child as the missing child while assessing the child's safety.
- (b) Gather available information about possible predators.
- (c) During the verification process, determine whether intervention services are needed to ensure that the child can safely remain in the home and ensure that arrangements are made for delivery of these services.
 - 1. These include, but are not limited to, our department's Victim's Service Advocates.
- (d) Complete the designated supplemental reports and cancel all outstanding notifications to include any NCIC Missing Person File entry and the State of Utah's Missing Children's Clearinghouse.
- (e) Supplemental reports should describe the child's activities while missing and the circumstances of the recovery/return.

318.8 WHEN A MISSING PERSON IS FOUND

When any person reported missing is found, the assigned investigator/responding officer shall document the location of the missing person in the appropriate report, conduct follow-up interview

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Missing Persons

with the missing located person, notify the relatives and/or reporting party, as appropriate, and other involved agencies, and refer the case for additional investigation if warranted. Notification to the appropriate division commander is required.

The Division Commander should ensure that, upon receipt of information that a missing person has been located, the following occurs:

- (a) Notification is made to the Utah BCI.
- (b) A missing child's school is notified.
- (c) Entries are made in the applicable missing person networks.
- (d) When a person is at risk, the fact that the person has been found should be reported within 24 hours to the Utah BCI.
- (e) Notification shall be made to any other law enforcement agency that took the initial report or participated in the investigation.

318.8.1 UNIDENTIFIED PERSONS

Department members investigating a case of an unidentified person who is deceased or a living person who cannot assist in identifying themselves should:

- (a) Obtain a complete description of the person.
- (b) Enter the unidentified person's description into the NCIC Unidentified Person File and the NamUs database.
- (c) Use available resources, such as those related to missing persons, to identify the person.

318.9 CASE CLOSURE

The Investigations Division supervisor may authorize the closure of a missing person case after considering the following:

- (a) Closure is appropriate when the missing person is confirmed returned or evidence matches an unidentified person or body.
- (b) If the missing person is a resident of South Salt Lake or this department is the lead agency, the case should be kept under active investigation for as long as the person may still be alive. Exhaustion of leads in the investigation should not be a reason for closing a case.
- (c) If this department is not the lead agency, the case can be made inactive if all investigative leads have been exhausted, the lead agency has been notified and entries are made in the applicable missing person networks, as appropriate.
- (d) A missing person case should not be closed or reclassified because the person would have reached a certain age or adulthood or because the person is now the subject of a criminal or civil warrant.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Missing Persons

318.10 TRAINING

Subject to available resources, the Investigations Supervisor should ensure that members of this department whose duties include missing person investigations and reports receive training that includes:

- (a) The initial investigation:
 - 1. Assessments and interviews
 - 2. Use of current resources, such as Mobile Audio Video (MAV)
 - 3. Confirming missing status and custody status of minors
 - 4. Evaluating the need for a heightened response
 - 5. Identifying the zone of safety based on chronological age and developmental stage
- (b) Briefing of department members at the scene.
- (c) Identifying NCIC Missing Person File categories (e.g., disability, endangered, involuntary, juvenile and catastrophe).
- (d) Verifying the accuracy of all descriptive information.
- (e) Initiating a neighborhood investigation.
- (f) Investigating any relevant recent family dynamics.
- (g) Addressing conflicting information.
- (h) Key investigative and coordination steps.
- (i) Managing a missing person case.
- (j) Additional resources and specialized services.
- (k) Update procedures for case information and descriptions.
- (l) Preserving scenes.
- (m) Internet and technology issues (e.g., Internet use, cell phone use).
- (n) Media relations.

Discriminatory Harassment

319.1 PURPOSE AND SCOPE

The purpose of this policy is to prevent department members from being subjected to discriminatory harassment, including sexual harassment and retaliation. Nothing in this policy is intended to create a legal or employment right or duty that is not created by law.

319.2 POLICY

The South Salt Lake Police Department is an equal opportunity employer and is committed to creating and maintaining a work environment that is free of all forms of discriminatory harassment, including sexual harassment and retaliation. The Department will not tolerate discrimination against employees in hiring, promotion, discharge, compensation, fringe benefits, and other privileges of employment. The Department will take preventive and corrective action to address any behavior that violates this policy or the rights and privileges it is designed to protect (Utah Antidiscrimination Act, Utah Code, Title 34A, Chapter 5).

The non-discrimination policies of the Department may be more comprehensive than state or federal law. Conduct that violates this policy may not violate state or federal law but still could subject an employee to discipline.

319.3 DEFINITIONS

Definitions related to this policy include:

319.3.1 DISCRIMINATION

The Department prohibits all forms of discrimination, including any employment-related action by a member that adversely affects an applicant or member and is based on actual or perceived race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, age, disability, pregnancy, genetic information, veteran status, marital status, and any other classification or status protected by law.

Discriminatory harassment, including sexual harassment, is verbal or physical conduct that demeans or shows hostility or aversion toward an individual based upon that individual's protected class. It has the effect of interfering with a member's work performance or creating a hostile or abusive work environment.

Conduct that may, under certain circumstances, constitute discriminatory harassment can include making derogatory comments; making crude and offensive statements or remarks; making slurs or off-color jokes; stereotyping; engaging in threatening acts; making indecent gestures, pictures, cartoons, posters, or material; making inappropriate physical contact; or using written material or department equipment and/or systems to transmit or receive offensive material, statements, or pictures. Such conduct is contrary to department policy and to a work environment that is free of discrimination.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Discriminatory Harassment

319.3.2 RETALIATION

Retaliation is treating a person differently or engaging in acts of reprisal or intimidation against the person because the person has engaged in protected activity, filed a charge of discrimination, participated in an investigation, or opposed a discriminatory practice. Retaliation will not be tolerated.

319.3.3 SEXUAL HARASSMENT

The Department prohibits all forms of discrimination and discriminatory harassment, including sexual harassment. It is unlawful to harass an applicant or a member because of that person's sex.

Sexual harassment includes but is not limited to unwelcome sexual advances, requests for sexual favors, or other verbal, visual, or physical conduct of a sexual nature when:

- (a) Submission to such conduct is made either explicitly or implicitly a term or condition of employment, position, or compensation.
- (b) Submission to, or rejection of, such conduct is used as the basis for any employment decisions affecting the member.
- (c) Such conduct has the purpose or effect of substantially interfering with a member's work performance or creating an intimidating, hostile, or offensive work environment.

319.3.4 ADDITIONAL CONSIDERATIONS

Discrimination and discriminatory harassment do not include actions that are in accordance with established rules, principles, or standards, including:

- (a) Acts or omission of acts based solely upon bona fide occupational qualifications under the Equal Employment Opportunity Commission (EEOC) and the Utah Anti-Discrimination and Labor Division.
- (b) Bona fide requests or demands by a supervisor that the member improve the member's work quality or output, that the member report to the job site on time, that the member comply with City or department rules or regulations, or any other appropriate work-related communication between supervisor and member.

319.4 RESPONSIBILITIES

This policy applies to all department members, who shall follow the intent of these guidelines in a manner that reflects department policy, professional standards, and the best interest of the Department and its mission.

Members are encouraged to promptly report any discriminatory, retaliatory, or harassing conduct or known violations of this policy to a supervisor. Any member who is not comfortable with reporting violations of this policy to the member's immediate supervisor may bypass the chain of command and make the report to a higher-ranking supervisor or manager. Complaints may also be filed with the Chief of Police, the Director of Human Services, or the Mayor.

Any member who believes, in good faith, that the member has been discriminated against, harassed, or subjected to retaliation, or who has observed harassment, discrimination, or

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Discriminatory Harassment

retaliation, is encouraged to promptly report such conduct in accordance with the procedures set forth in this policy.

Supervisors and managers receiving information regarding alleged violations of this policy shall determine if there is any basis for the allegation and shall proceed with resolution as stated below.

319.4.1 SUPERVISOR RESPONSIBILITIES

The responsibilities of supervisors and managers shall include but are not limited to:

- (a) Continually monitoring the work environment and striving to ensure that it is free from all types of unlawful discrimination, including sexual harassment or retaliation.
- (b) Taking prompt, appropriate action within their work units to avoid and minimize the incidence of any form of discrimination, harassment, or retaliation.
- (c) Ensuring that their subordinates understand their responsibilities under this policy.
- (d) Ensuring that members who make complaints or who oppose any unlawful employment practices are protected from retaliation and that such matters are kept confidential to the extent possible.
- (e) Making a timely determination regarding the substance of any allegation based upon all available facts.
- (f) Notifying the Chief of Police or the Director of Human Services in writing of the circumstances surrounding any reported allegations or observed acts of discrimination, harassment or retaliation no later than the next business day.

319.4.2 SUPERVISOR'S ROLE

Supervisors and managers shall be aware of the following:

- (a) Behavior of supervisors and managers should represent the values of the Department and professional standards.
- (b) False or mistaken accusations of discrimination, harassment or retaliation have negative effects on the careers of innocent members.

Nothing in this section shall be construed to prevent supervisors or managers from discharging supervisory or management responsibilities, such as determining duty assignments, evaluating or counseling employees, or issuing discipline in a manner that is consistent with established procedures.

319.4.3 QUESTIONS OR CLARIFICATION

Members with questions regarding what constitutes discrimination, sexual harassment, or retaliation are encouraged to contact a supervisor, a manager, the Chief of Police, the Director of Human Services, the Mayor, or legal for further information, direction, or clarification.

319.5 INVESTIGATION OF COMPLAINTS

Various methods of resolution exist. During the pendency of any such investigation, the supervisor of the involved members should take prompt and reasonable steps to mitigate or eliminate any continuing abusive or hostile work environment. It is the policy of the Department that all

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Discriminatory Harassment

complaints of discrimination, retaliation, or harassment shall be fully documented, and promptly and thoroughly investigated.

319.5.1 SUPERVISOR RESOLUTION

Members who believe they are experiencing discrimination, harassment, or retaliation should be encouraged to inform the individual that the behavior is unwelcome, offensive, unprofessional, or inappropriate. However, if the member feels uncomfortable or threatened or has difficulty expressing the member's concern, or if this does not resolve the concern, assistance should be sought from a supervisor or manager who is a rank higher than the alleged transgressor.

319.5.2 FORMAL INVESTIGATION

If the complaint cannot be satisfactorily resolved through the process described above, a formal investigation will be conducted.

The person assigned to investigate the complaint will have full authority to investigate all aspects of the complaint. Investigative authority includes access to records and the cooperation of any members involved. No influence will be used to suppress any complaint and no member will be subject to retaliation or reprisal for filing a complaint, encouraging others to file a complaint or for offering testimony or evidence in an investigation.

Formal investigation of the complaint will be confidential to the extent possible and will include but is not limited to details of the specific incident, frequency and dates of occurrences and names of any witnesses. Witnesses will be advised regarding the prohibition against retaliation, and that a disciplinary process, up to and including termination, may result if retaliation occurs.

Members who believe they have been discriminated against, harassed, or retaliated against because of their protected status are encouraged to follow the chain of command but may also file a complaint directly with the Chief of Police, the Director of Human Services, or the Mayor.

319.5.3 ALTERNATIVE COMPLAINT PROCESS

No provision of this policy shall be construed to prevent any member from seeking legal redress outside the Department. Members who believe that they have been harassed, discriminated against, or retaliated against are entitled to bring complaints of employment discrimination to federal, state, and/or local agencies responsible for investigating such allegations. Specific time limitations apply to the filing of such charges. Members are advised that proceeding with complaints under the provisions of this policy does not in any way affect those filing requirements.

319.6 DOCUMENTATION OF COMPLAINTS

All complaints or allegations shall be thoroughly documented on the appropriate forms and in a manner designated by the Chief of Police. The outcome of all reports shall be:

- Approved by the Chief of Police, the Mayor, or the Director of Human Services, depending on the ranks of the involved parties.
- Maintained in accordance with the established records retention schedule.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Discriminatory Harassment

319.6.1 NOTIFICATION OF DISPOSITION

The complainant and/or victim will be notified in writing of the disposition of the investigation and the action taken to remedy or address the circumstances giving rise to the complaint.

319.7 TRAINING

All new members shall be provided with a copy of this policy as part of their orientation. The policy shall be reviewed with each new member. The member shall certify by signing the prescribed form that the member has been advised of this policy, is aware of and understands its contents, and agrees to abide by its provisions during the member's term with the Department.

All members shall receive annual training on the requirements of this policy and shall certify by signing the prescribed form that they have reviewed the policy, understand its contents, and agree that they will continue to abide by its provisions.

Child Abuse

320.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the investigation of suspected child abuse. This policy also addresses when South Salt Lake Police Department members are required to notify the Division of Child and Family Services (DCFS) of suspected child abuse.

320.1.1 DEFINITIONS

Definitions related to this policy include:

Child - Unless otherwise specified by a cited statute, a child is any person under the age of 18 years.

Child abuse - Non-accidental harm (e.g., physical, emotional, developmental injury or damage) or threatened harm of a child (e.g., actions, inactions, credible verbal threats, indicating that the child is at an unreasonable risk of harm or neglect), sexual abuse (e.g., bigamy, incest), sexual exploitation of a child, human trafficking of a child, or causing the intentional death of the child's parent by the child's parent as defined by Utah law (e.g., specified parent-child relationships). Abuse does not include reasonable discipline, restraint, weapon removal, or management of a child or other legally justifiable acts (Utah Code 80-1-102).

320.2 POLICY

The South Salt Lake Police Department will investigate all reported incidents of alleged criminal child abuse and ensure DCFS is notified as required by law.

320.3 MANDATORY NOTIFICATION

Members of the South Salt Lake Police Department shall notify DCFS when there is reason to believe that a child has been subjected to child abuse, when they observe a child being subjected to conditions or circumstances that would reasonably result in child abuse, or when any person notifies the member of child abuse (Utah Code 80-2-602).

320.3.1 NOTIFICATION PROCEDURE

Notification should be made as soon as practicable to the nearest DCFS office (Utah Code 80-2-602).

Notification should also be made to the District Attorney in cases where suspected child abuse resulted in death (Utah Code 80-2-604).

320.4 QUALIFIED INVESTIGATORS

Qualified investigators should be available for child abuse investigations. These investigators should:

- (a) Conduct interviews in child appropriate interview facilities.
- (b) Be familiar with forensic interview techniques specific to child abuse investigations.
- (c) Present all cases of alleged child abuse to the prosecutor for review.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Child Abuse

- (d) Coordinate with other enforcement agencies, social service agencies and school administrators as needed.
- (e) Provide referrals to therapy services, victim advocates, guardians and support for the child and family as appropriate.
- (f) Participate in or coordinate with multidisciplinary investigative teams as applicable.

320.5 INVESTIGATIONS AND REPORTING

In all reported or suspected cases of child abuse, officers shall write a report even if the allegations appear unfounded or unsubstantiated.

Investigations and reports related to suspected cases of child abuse should address, as applicable:

- (a) The overall basis for the contact. This should be done by the investigating officer in all circumstances where a suspected child abuse victim was contacted.
- (b) The exigent circumstances that existed if officers interviewed the child victim without the presence of a parent or guardian.
- (c) Any relevant statements the child may have made and to whom he/she made the statements.
- (d) If a child was taken into protective custody, the reasons, the name and title of the person making the decision, and why other alternatives were not appropriate.
- (e) Documentation of any visible injuries or any injuries identified by the child. This should include photographs of such injuries, if practicable.
- (f) Whether the child victim was transported for medical treatment or a medical examination.
- (g) Whether the victim identified a household member as the alleged perpetrator, and a list of the names of any other children who may reside in the residence.
- (h) Identification of any prior related reports or allegations of child abuse, including other jurisdictions, as reasonably known.
- (i) Previous addresses of the victim and suspect.
- (j) Other potential witnesses who have not yet been interviewed, such as relatives or others close to the victim's environment.

All cases of the unexplained death of a child should be investigated as thoroughly as if it had been a case of suspected child abuse (e.g., a sudden or unexplained death of an infant).

320.5.1 COMMERCIAL SEX OR SEXUAL SOLICITATION INVOLVING A CHILD

When an officer encounters a child engaged in commercial sex or sexual solicitation, the officer should (Utah Code 76-5d-106):

- (a) Investigate possible human trafficking of the child.
- (b) Refer the child to DCFS.
- (c) Bring the child to a receiving center.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Child Abuse

- (d) Contact the child's parent or guardian.

320.6 PROTECTIVE CUSTODY

Before taking any child into protective custody, the officer should make reasonable attempts to contact DCFS. Generally, removal of a child from the child's family, guardian, or other responsible adult should be left to the child welfare authorities when they are present or have become involved in an investigation.

Generally, members of this [department/office] should remove a child from the child's parent or guardian without a court order only when no other effective alternative is reasonably available and immediate action reasonably appears necessary to protect the child. Prior to taking a child into protective custody, the officer should take reasonable steps to deliver the child to another qualified parent or legal guardian, unless it reasonably appears that the release would endanger the child or result in abduction. If this is not a reasonable option, the officer shall ensure that the child is delivered to DCFS.

Whenever practicable, the officer should inform a supervisor of the circumstances prior to taking a child into protective custody. If prior notification is not practicable, officers should contact a supervisor promptly after taking a child into protective custody.

Children may only be removed from a parent or guardian in the following situations (Utah Code 80-2a-202):

- (a) When a court order has been issued authorizing the removal of the child.
- (b) Without a court order, when there exist exigent circumstances sufficient to relieve an officer of the requirement to obtain a warrant.
- (c) Without a warrant when an officer obtains the consent of the child's parent or guardian.

The above apply to removing a child from a home or school as well as from a parent or guardian.

320.6.1 NOTICE AFTER PROTECTIVE CUSTODY

An officer who takes a child into protective custody shall immediately use reasonable efforts to locate and inform, through the most efficient means available, the child's parents, non-custodial parents, guardian, or responsible relative of the information set forth in Utah Code 80-2a-203. This notice should include the written information prepared by DCFS. Such efforts to provide this notification should be documented in the related report.

320.7 INTERVIEWS

320.7.1 PRELIMINARY INTERVIEWS

Absent extenuating circumstances or impracticality, officers should record the preliminary interview with suspected child abuse victims. Officers should avoid multiple interviews with a child victim and should attempt to gather only the information necessary to begin an investigation. When practicable, investigating officers should defer interviews until a person who is specially trained in such interviews is available. Generally, child victims should not be interviewed in the home or location where the alleged abuse occurred.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Child Abuse

320.7.2 DETAINING SUSPECTED CHILD ABUSE VICTIMS FOR AN INTERVIEW

An officer should not detain a child involuntarily who is suspected of being a victim of child abuse solely for the purpose of an interview or physical exam without the consent of a parent or guardian unless one of the following applies:

- (a) Exigent circumstances exist, such as:
 - 1. A reasonable belief that medical issues of the child need to be addressed immediately.
 - 2. A reasonable belief that the child is or will be in danger of harm if the interview or physical exam is not immediately completed.
 - 3. The alleged offender is the custodial parent or guardian and there is reason to believe the child may be in continued danger.
- (b) A court order or warrant has been issued.

320.7.3 INTERVIEWS OF CHILDREN IN STATE CUSTODY

Officers should not interview a child who is in the custody of DCFS without the consent of the child's guardian ad litem. If a guardian ad litem has not been appointed, consent may be given by DCFS (Utah Code 80-2-705).

320.8 MEDICAL EXAMINATIONS

If the child has been the victim of abuse that requires a medical examination, the investigating officer should obtain consent for such examination from the appropriate parent, guardian or agency having legal custody of the child. The officer should also arrange for the child's transportation to the appropriate medical facility.

In cases where the alleged offender is the custodial parent or guardian and is refusing consent for the medical examination, officers should notify a supervisor before proceeding. If exigent circumstances do not exist or if state law does not provide for officers to take the child for a medical examination, the notified supervisor should consider obtaining a court order for such an examination.

320.9 DRUG-ENDANGERED CHILDREN

A coordinated response by law enforcement and social services agencies is appropriate to meet the immediate and longer-term medical and safety needs of children exposed to the manufacturing, trafficking or use of narcotics.

320.9.1 SUPERVISOR RESPONSIBILITIES

The Investigations Division Supervisor should:

- (a) Work with professionals from the appropriate agencies, including DCFS, other law enforcement agencies, medical service providers and local prosecutors to develop community specific procedures for responding to situations where there are children endangered by exposure to methamphetamine labs or the manufacture and trafficking of other drugs.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Child Abuse

- (b) Activate any available interagency response when an officer notifies the Investigations Division Supervisor that the officer has responded to a drug lab or other narcotics crime scene where a child is present or where evidence indicates that a child lives there.
- (c) Develop a report format or checklist for use when officers respond to drug labs or other narcotics crime scenes. The checklist will help officers document the environmental, medical, social and other conditions that may affect the child.

320.9.2 OFFICER RESPONSIBILITIES

Officers responding to a drug lab or other narcotics crime scene where a child is present or where there is evidence that a child lives should:

- (a) Document the environmental, medical, social and other conditions of the child using photography as appropriate and the checklist or form developed for this purpose.
- (b) Notify the Investigations Division Supervisor so an interagency response can begin.

320.10 STATE MANDATES AND OTHER RELEVANT LAWS

Utah requires or permits the following:

320.10.1 RELEASE OF REPORTS

Information related to incidents of child abuse or suspected child abuse shall be confidential and may only be disclosed pursuant to state law and the Records Maintenance and Release Policy (Utah Code 77-37-4; Utah Code 80-2-608).

320.10.2 RECORDED INTERVIEWS

A parent or guardian of a child victim may view a recorded interview of the child unless (Utah Code 77-37-4):

- (a) The suspect is also a parent or guardian of the child victim;
- (b) The suspect resides in the home with the child victim; or
- (c) The investigator reasonably believes that allowing the parent or guardian to review the recording would compromise or impede the investigation.

The investigator should coordinate with the Children's Justice Center to ensure the viewing takes place within two business days of the request.

320.10.3 RETENTION REQUIREMENTS

Recordings of any interview of a child during the investigation of an allegation of any sexual abuse of the child shall be retained for 18 years following the date of the last recording, unless the prosecuting attorney requests in writing that the recording be retained for an additional period of time (Utah Code 53-13-110.5).

320.10.4 NOTIFICATION UPON ARREST OR ISSUANCE OF A CITATION

When an officer arrests or issues a citation to a person 18 years of age or older for child abuse, the officer shall provide the individual with the written notice required by Utah Code 78B-7-802. Victims shall be provided notice in accordance with the Victim and Witness Assistance Policy.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Child Abuse

320.11 TRAINING

The [Department/Office] should provide training on best practices in child abuse investigations to members tasked with investigating these cases. The training should include:

- (a) Participating in multidisciplinary investigations, as appropriate.
- (b) Conducting forensic interviews.
- (c) Availability of therapy services for children and families.
- (d) Availability of specialized forensic medical exams.
- (e) Cultural competence (including interpretive services) related to child abuse investigations.
- (f) Availability of victim advocate or guardian ad litem support.

Report Preparation

321.1 PURPOSE AND SCOPE

Report preparation is a major part of each officer's job. The purpose of reports is to document sufficient information to refresh the officer's memory and to provide factual detailed information for follow-up investigation and successful prosecution. Report writing is the subject of substantial formalized training and on-the-job training.

321.1.1 REPORT PREPARATION

Employees should ensure that reports are sufficiently detailed for their purpose and free from errors prior to submission. It is the responsibility of the assigned employee to complete and submit all reports taken during the shift before going off-duty unless permission to hold the report has been approved by a supervisor. Generally, reports requiring prompt follow-up action on active leads, or arrest reports where the suspect remains in custody should not be held.

Handwritten reports must be prepared legibly. If the report is not legible, the submitting employee will be required by the reviewing supervisor to promptly make corrections and resubmit the report. Employees who dictate reports shall use appropriate grammar, as content is not the responsibility of the typist. Employees who generate reports on computers are subject to all requirements of this policy.

All reports shall accurately reflect the identity of the persons involved, all pertinent information seen, heard or assimilated by any other sense, and any actions taken. Employees shall not suppress, conceal or distort the facts of any reported incident, nor shall any employee make a false report orally or in writing. Generally, the reporting employee's opinions should not be included in reports unless specifically identified as such.

321.2 REQUIRED REPORTING

Written reports are required in all of the following situations on the appropriate Department-approved form unless otherwise approved by a supervisor.

321.2.1 CRIMINAL ACTIVITY

When a member responds to a call for service, or as a result of self-initiated activity becomes aware of any activity where a crime has occurred, the member shall document the incident regardless of whether a victim desires prosecution.

Activity to be documented in a written report includes:

- (a) All arrests
- (b) All felony crimes
- (c) Non-felony incidents involving threats or stalking behavior
- (d) Situations covered by separate policy. These include:
 - 1. Use of Force Policy

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Report Preparation

2. Domestic Violence Policy
3. Child Abuse Policy
4. Adult Abuse Policy
5. Hate Crimes Policy
6. Suspicious Activity Reporting Policy

- (e) All misdemeanor crimes where the victim desires a report

Misdemeanor crimes where the victim does not desire a report shall be documented using the department-approved alternative reporting method (e.g., dispatch log).

321.2.2 NON-CRIMINAL ACTIVITY

The following incidents shall be documented using the appropriate approved report:

- (a) Any time an officer points a firearm at any person
- (b) Any use of force against any person by a member of this department (see the Use of Force Policy)
- (c) Any firearm discharge (see the Firearms Policy)
- (d) Any time a person is reported missing, regardless of jurisdiction (see the Missing Persons Policy)
- (e) Any found property or found evidence
- (f) Any traffic collision above the minimum reporting level (see the Traffic Collision Reporting Policy)
- (g) Suspicious incidents that may indicate a potential for crimes against children or that a child's safety is in jeopardy
- (h) All protective custody detentions
- (i) Suspicious incidents that may place the public or others at risk
- (j) Whenever the employee believes the circumstances should be documented or at the direction of a supervisor

321.2.3 DEATH CASES

Death investigations require specific investigation methods depending on circumstances and should be handled in accordance with the Death Investigation Policy. An officer handling a death investigation should notify and apprise a supervisor of the circumstances surrounding the incident and a determination will be made on how to proceed. The following cases shall be appropriately investigated and documented using the approved report:

- (a) Sudden or accidental deaths
- (b) Suicides

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Report Preparation

- (c) Homicide or suspected homicide
- (d) Unattended deaths (no physician or qualified hospice care in the 30 days preceding death)
- (e) Found dead bodies or body parts

321.2.4 INJURY OR DAMAGE BY SOUTH SALT LAKE PERSONNEL

Reports shall be taken if an injury occurs that is a result of an act of a City employee. Additionally, reports shall be taken involving damage to City property or City equipment.

If the injury or damage is significant, or may expose the City to potential liability, a supervisor should be notified. Supervisors notified of such events should consider requesting an investigation by an allied agency, notification of the Chief of Police via chain of command and involvement of City Risk Management assistance.

321.2.5 MISCELLANEOUS INJURIES

Any injury that is reported to this department shall require a report when:

- (a) The injury is a result of drug overdose.
- (b) Attempted suicide.
- (c) The injury is major/serious, whereas death could result.
- (d) The circumstances surrounding the incident are suspicious in nature and it is desirable to record the event.

The above reporting requirements are not intended to be all inclusive. A supervisor may direct an employee to document any incident he/she deems necessary.

321.3 EXPEDITIOUS REPORTING

In general, all officers and supervisors shall act with promptness and efficiency in the preparation and processing of all reports. An incomplete report, unorganized reports or report completions delayed without supervisory approval are not acceptable. Reports should be submitted by the end of shift and processed according to established priorities or according to special priority necessary under exceptional circumstances. If the required report is unable to be completed prior to end of shift the immediate supervisor should be notified of circumstance.

321.3.1 HANDWRITTEN REPORTS

Some incidents and report forms lend themselves to block print rather than typing. In general, the narrative portion of those reports where an arrest is made or when there is a long narrative should be typed or dictated.

Supervisors may require block printing or typing of reports of any nature for Department consistency.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Report Preparation

321.3.2 GENERAL USE OF OTHER HANDWRITTEN FORMS

County, state and federal agency forms may be block printed as appropriate. In general, the form, by design, may require typing.

321.4 REPORT CORRECTIONS

Supervisors shall review reports for content and accuracy. Supervisors shall check codes, NBIRS, required fields and narrative for verification of thorough and complete report submission. If a correction is necessary, the reviewing supervisor should reject/send back the report in the correction queue with notes explaining the correction need. The submitting officer should address the correction concerns timely.

321.5 REPORT CHANGES OR ALTERATIONS

Reports that have been approved by a supervisor and submitted to the Records Section for filing and distribution shall not be modified or altered except by way of a supplemental report. Reviewed reports that have not yet been submitted to the Records Section may be corrected or modified by the authoring officer only with the knowledge and authorization of the reviewing supervisor.

321.6 ELECTRONIC SIGNATURES

The South Salt Lake Police Department has established an electronic signature procedure for use by all employees of the South Salt Lake Police Department. The Patrol Lieutenant shall be responsible for maintaining the electronic signature system and ensuring that each employee creates a unique, confidential password for his/her electronic signature.

- Employees may only use their electronic signatures for official reports or other official communications.
- Each employee shall be responsible for the security and use of his/her electronic signature and shall promptly notify a supervisor if the electronic signature has or may have been compromised or misused.

Media Relations

322.1 PURPOSE AND SCOPE

This policy provides guidelines for the release of official department information to the media. It also addresses coordinating media access to scenes of disasters, criminal investigations, emergencies and other law enforcement activities.

322.2 RESPONSIBILITIES

The ultimate authority and responsibility for the release of information to the media shall remain with the Chief of Police. In situations not warranting immediate notice to the Chief of Police and in situations where the Chief of Police has given prior approval, Division Commanders, Watch Commanders, and designated Public Information Officers (PIOs) may prepare and release information to the media in accordance with this policy and the applicable laws regarding confidentiality.

322.3 ACCESS

Authorized media representatives shall be provided access to scenes of disasters, criminal investigations, emergencies, and other law enforcement activities as required by law.

Access by the media is subject to the following conditions:

- (a) The media representative shall produce valid media credentials that shall be prominently displayed at all times while in areas otherwise closed to the public.
- (b) Media representatives should be prevented from interfering and may be removed for interfering with emergency operations and criminal investigations.
 - 1. Based upon available resources, reasonable effort should be made to provide a safe staging area for the media that is near the incident and that will not interfere with emergency or criminal investigation operations. All information released to the media should be coordinated through the PIO or other designated spokesperson.
- (c) Media interviews with individuals who are in custody should not be permitted without the approval of the Chief of Police and the express written consent of the person in custody.
- (d) No member of this [department/office] who is under investigation shall be subjected to media visits or interviews without the consent of the involved member.

322.3.1 CRITICAL OPERATIONS

A critical incident or tactical operation should be handled in the same manner as a crime scene, except the media should not be permitted within the inner perimeter of the incident, subject to any restrictions as determined by the supervisor in charge. Department members shall not jeopardize a critical incident or tactical operation in order to accommodate the media. All comments to the media shall be coordinated through a supervisor or the PIO.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Media Relations

322.3.2 TEMPORARY FLIGHT RESTRICTIONS

Whenever the presence of media or other aircraft pose a threat to public or member safety or significantly hamper incident operations, the field supervisor should consider requesting a Temporary Flight Restriction (TFR). All requests for a TFR should be routed through the Watch Commander. The TFR request should include specific information regarding the perimeter and altitude necessary for the incident and should be requested through the appropriate control tower. If the control tower is not known, the Federal Aviation Administration (FAA) should be contacted (14 CFR 91.137).

322.4 CONFIDENTIAL OR RESTRICTED INFORMATION

It shall be the responsibility of the PIO to ensure that confidential or restricted information is not inappropriately released to the media (see the Records Maintenance and Release and Personnel Records policies). When in doubt, authorized and available legal counsel should be consulted prior to releasing any information.

322.4.1 EMPLOYEE INFORMATION

The identities of officers involved in shootings or other critical incidents may only be released to the media upon the consent of the involved officer or upon a formal request filed.

Any requests for copies of related reports or additional information not contained in the information log (see the Information Log section in this policy), including the identity of officers involved in shootings or other critical incidents, shall be referred to the PIO.

Requests should be reviewed and fulfilled by the Records Officer, or if unavailable, the Watch Commander or the authorized designee. Such requests will be processed in accordance with the provisions of the Records Maintenance and Release Policy and public records laws (e.g., Government Records Access and Management Act).

322.4.2 PUBLIC STATEMENTS OR APPEARANCES - DEPARTMENT EMPLOYEES

Employees shall not address public gatherings, appear on radio or television, prepare any articles for publication, act as correspondents to the newspaper or periodicals without the prior approval of the Chief of Police or his/her designee. Exceptions would be interviews conducted with the departments assigned public information officer or interviews conducted at an incident scene.

322.4.3 INFORMATION PERTAINING TO ON-GOING CRIMINAL INVESTIGATIONS

- (a) The following list includes, but is not limited to, information that could compromise an active investigation, and shall not be released to the media without the express authorization of the Chief of Police or his/her designee.
 - 1. Prior criminal record of a suspect/defendant, including arrest, indictments, or other charges of criminal activity.
 - 2. Opinions or other statements as to the character, reputation, guilt, or innocence of the accused.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Media Relations

3. Existence or contents of any confession, admission, alibis, or other statements of the accused, or the refusal or failure of the accused to make any such statements.
 4. Performance or results of investigative procedures or tests, such as fingerprints, polygraph examination, ballistic test, or other laboratory tests or examinations, or the refusal of the accused to take such tests or examinations.
 5. Statements or opinions concerning the identity, address, testimony, or credibility of prospective witness(es).
 6. Speculation regarding plea-bargaining or other disposition of the charge or case.
 7. Statements or opinions concerning evidence, physical or oral, or argument in the case, or whether or not it is anticipated such evidence or argument will be used at trial.
 8. Name or location of the accused's employment, except if the location of the crime or arrest is the same.
 9. Name or address of any victim of a sex offense. Only the approximate location of where the offense took place should be released.
 10. Name of juveniles suspected or arrested.
 11. Exact amount of cash or specific description of any items taken in a robbery or burglary, unless a detailed description is needed to assist in recovery.
- (b) Inquiries regarding a victim in a death investigation will only be answered after a death notification has been made to the next of kin, or after a reasonable attempt has been made as determined by the on-scene commander.
- (c) Any information concerning an internal investigation, including the existence of such an investigation, without the express authorization of the Chief of Police.
- (d) Anyone asking for information that may not be made public will be granted an explanation of why the information is being withheld. For example, explaining rights to privacy and the necessity for avoiding prejudicial pretrial publicity.

322.4.4 MINOR VICTIMS OF CRIMINAL HOMICIDE

The [Department/Office] should not release the name or the personal identifying information of a minor victim of a criminal homicide to the media until reasonable steps have been taken to obtain the consent of the victim's parent or legal guardian to release the information (Utah Code 53-25-101).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Media Relations

322.4.5 ONGOING CRIMINAL INVESTIGATIONS

Media requests for information about an ongoing criminal investigation should be evaluated by the Investigations Division supervisor, and the PIO. If a release of information could reasonably be expected to interfere with the investigation, the information shall not be released.

322.5 POLICY

It is the policy of the South Salt Lake Police Department to protect the privacy rights of individuals, while releasing non-confidential information to the media regarding topics of public concern. Information that has the potential to negatively affect investigations will not be released.

322.6 PROVIDING ADVANCE INFORMATION

To protect the safety and rights of department members and other persons, advance information about planned actions by law enforcement personnel, such as movement of persons in custody or the execution of an arrest or search warrant, should not be disclosed to the media, nor should media representatives be invited to be present at such actions except with the prior approval of the Chief of Police.

Any exceptions to the above should only be considered for the furtherance of legitimate law enforcement purposes. Prior to approving any exception, the Chief of Police will consider, at a minimum, whether the release of information or the presence of the media would unreasonably endanger any individual or prejudice the rights of any person or is otherwise prohibited by law.

322.7 MEDIA REQUESTS

Any media request for information or access to a law enforcement incident shall be referred to the PIO, or if unavailable, to the first available supervisor. Prior to releasing any information to the media, members shall consider the following:

- (a) At no time shall any member of this department make any comment or release any official information to the media without prior approval from a supervisor or the PIO.
- (b) In situations involving multiple agencies or government departments, every reasonable effort should be made to coordinate media releases with the authorized representative of each involved agency prior to the release of any information by this department.
- (c) Under no circumstance should any member of this department make any comment to the media regarding any law enforcement incident not involving this department without prior approval of the Chief of Police. Under these circumstances the member should direct the media to the agency handling the incident.

322.8 RELEASE OF INFORMATION

The Department may routinely release information to the media without receiving a specific request. This may include media releases regarding critical incidents, information of public concern, updates regarding significant incidents or requests for public assistance in solving crimes or identifying suspects. This information may also be released through the department website or other electronic data sources.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Media Relations

322.8.1 INFORMATION LOG

The Department will maintain a daily information log of significant law enforcement activities. Log entries shall only contain information that is deemed public information and not restricted or confidential by this policy or applicable law. Upon request, the log entries shall be made available to media representatives through the Watch Commander.

The daily information log will generally include:

- (a) The date, time, location, case number, type of crime, extent of injury or loss, and names of individuals involved in crimes occurring within this jurisdiction, unless the release of such information would endanger the safety of any individual or jeopardize the successful completion of any ongoing investigation, or the information is confidential (e.g., juveniles or certain victims).
- (b) The date, time, location, case number, name, birth date and charges for each person arrested by this department, unless the release of such information would endanger the safety of any individual or jeopardize the successful completion of any ongoing investigation or the information is confidential (e.g., juveniles).
- (c) The time and location of other significant law enforcement activities or requests for service with a brief summary of the incident.

Subpoenas and Court Appearances

323.1 PURPOSE AND SCOPE

This policy establishes the guidelines for department members who must appear in court. It will allow the South Salt Lake Police Department to cover any related work absences and keep the Department informed about relevant legal matters.

323.2 POLICY

South Salt Lake Police Department members will respond appropriately to all subpoenas and any other court-ordered appearances.

323.2.1 SERVICE OF SUBPOENA

Service of a subpoena requiring the appearance of any Department employee in connection with a matter arising out of the employee's course and scope of official duties is accomplished by electronic service upon the employee and by emailing a cc: copy of the subpoena to the employee's supervisor or other authorized Department agent. Receipt of the service of the subpoena will be kept on the F: drive showing the receipt of service from both the employee and their respective supervisor. Subpoena service is also acceptable by courier or court liaison from the court to this Department.

323.3 SUBPOENAS

Only department members authorized to receive a subpoena on behalf of this department or any of its members may do so.

Criminal subpoenas may be served upon a member in accordance with U. R. Crim. P. Rule 14 by personally delivering a copy of the subpoena to the member.

Civil subpoenas may be served upon a member personally, by leaving a copy at the member's residence with a person of suitable age and discretion who resides there, or by delivering a copy to an agent authorized by appointment or by law to receive process. The subpoena may also be served by mail, commercial courier service or electronic delivery (U. R. Civ. P. Rule 45; U. R. Civ. P. Rule 4). Civil subpoenas shall not be accepted without properly posted fees (U. R. Civ. P. Rule 45).

323.3.1 SPECIAL NOTIFICATION REQUIREMENTS

Any member who is subpoenaed to testify, agrees to testify or provides information on behalf of or at the request of any party other than the City Attorney or the prosecutor shall notify his/her immediate supervisor without delay regarding:

- (a) Any civil case where the City or one of its members, as a result of his/her official capacity, is a party.
- (b) Any civil case where any other city, county, state or federal unit of government or a member of any such unit of government, as a result of his/her official capacity, is a party.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Subpoenas and Court Appearances

- (c) Any criminal proceeding where the member is called to testify or provide information on behalf of the defense.
- (d) Any civil action stemming from the member's on-duty activity or because of his/her association with the South Salt Lake Police Department.
- (e) Any personnel or disciplinary matter when called to testify or to provide information by a government entity other than the South Salt Lake Police Department.

The supervisor will then notify the Chief of Police and the appropriate prosecuting attorney as may be indicated by the case. The Chief of Police should determine if additional legal support is necessary.

No member shall be retaliated against for testifying in any matter.

323.3.2 CIVIL SUBPOENA

The Department will compensate members who appear in their official capacities on civil matters arising out of their official duties, as directed by the current memorandum of understanding or collective bargaining agreement.

The Department should seek reimbursement for the member's compensation through the civil attorney of record who subpoenaed the member.

323.3.3 OFF-DUTY RELATED SUBPOENAS

Members receiving valid subpoenas for off-duty actions not related to their employment or appointment will not be compensated for their appearance. Arrangements for time off shall be coordinated through their immediate supervisors.

323.4 FAILURE TO APPEAR

Any member who fails to comply with the terms of any properly served subpoena or court-ordered appearance may be subject to discipline. This includes properly served orders to appear that were issued by a state administrative agency.

323.5 STANDBY

To facilitate standby agreements, members are required to provide and maintain current information on their addresses and contact telephone numbers with the Department.

If a member on standby changes his/her location during the day, the member shall notify the designated department member of how he/she can be reached. Members are required to remain on standby until released by the court or the party that issued the subpoena.

323.6 COURTHOUSE PROTOCOL

When appearing in court, members shall:

- (a) Be punctual and prepared to proceed immediately with the case for which they are scheduled to appear.
- (b) Dress in the department uniform or business attire.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Subpoenas and Court Appearances

- (c) Observe all rules of the court in which they are appearing and remain alert to changes in the assigned courtroom where their matter is to be heard.

323.6.1 TESTIMONY

Before the date of testifying, the subpoenaed member shall request a copy of relevant reports and become familiar with the content in order to be prepared for court.

323.7 OVERTIME

When a member appears in court on his/her off-duty time, he/she will be compensated in accordance with the current memorandum of understanding or collective bargaining agreement.

Reserve and Auxiliary Officers

324.1 PURPOSE AND SCOPE

The South Salt Lake Police Department Reserve Unit was established to supplement and assist regular sworn police officers in their duties. This unit provides professional, sworn volunteer reserve officers who can augment regular staffing levels. For the purposes of this policy, "Reserve" includes reserve and auxiliary officers unless specifically described otherwise.

324.1.1 DEFINITIONS

Sworn - Means having taken the oath of office set forth in Utah Constitution Article IV, Section 10, administered by the law enforcement agency for which a peace officer works.

Reserve Officer - Means a sworn and certified peace officer, whether paid or voluntary, who:

- (a) Is serving in a reserve capacity for a law enforcement agency that is part of or administered by the state or any of its political subdivisions.
- (b) Meets the basic and in-service training requirements of the peace officer classification in which the officer will function (Utah Code 53-13-111(3)).

Auxiliary Officer - Means a sworn, certified, and supervised special function officer, as described by Utah Code 53-13-112 and is a specific category of special function officer required to have the level of training of a special function officer as provided in Utah Code 53-13-105, including no fewer than 40 hours per year of in-service training (Utah Code 53-13-101; Utah Code 53-13-112).

Volunteer - Means an officer who donates service without pay or other compensation except expenses actually and reasonably incurred as approved by the supervising agency.

While on-duty - Means while an officer is actually performing the job duties and work activities assigned by the employing agency and for which the officer is trained and certified, and may include time spent outside those duties and activities if that additional time involves an activity that is an integral and necessary part of the job, and is spent for the benefit, and under the direction of, the employing agency (Utah Code 53-13-101(14)(a)). "While on-duty" does not include the time an officer spends commuting between home and place of employment unless that time involves an on-duty activity identified in Utah Code 53-13-101(14)(a) (Utah Code 53-13-101(14)(b)).

324.2 SELECTION AND APPOINTMENT OF POLICE RESERVE OFFICERS

The South Salt Lake Police Department shall endeavor to recruit and appoint to the Reserve Unit only those applicants who meet the high ethical, moral and professional standards set forth by this Department.

324.2.1 PROCEDURE

All applicants shall be required to meet and pass the same pre-employment procedures as regular police officers before appointment, including any state and or Police Officer Standards and Training (POST) requirements.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Reserve and Auxiliary Officers

324.2.2 APPOINTMENT

Applicants who are selected for appointment to the Police Reserve Unit shall, on the recommendation of the Chief of Police, be sworn in by the Chief of Police and take a loyalty oath to observe and obey all of the laws of the land and to carry out their duties to the best of their abilities.

The Department may utilize a sworn and certified peace officer in a reserve or auxiliary capacity (Utah Code 53-13-111(1)(a)).

324.2.3 COMPENSATION FOR POLICE RESERVE OFFICERS

Compensation for reserve officers is provided as follows:

While serving as a non-paid volunteer in a reserve or auxiliary capacity, or working part-time for fewer hours than would qualify the officer as an "employee" under state or federal law, a peace officer is entitled to benefits in accordance with Utah Code, Title 67, Chapter 20, Volunteer Government Workers Act (Utah Code 53-13-111(2)).

All reserve officer appointees are issued two sets of uniforms and all designated attire and safety equipment. All property issued to the reserve officer shall be returned to the [Department/Office] upon termination or resignation. Reserves shall receive a yearly uniform allowance equal to that of regular officers.

324.2.4 EMPLOYEES WORKING AS RESERVE OFFICERS

Qualified employees of this department, when authorized, may also serve as reserve officers. However, the Department must not utilize the services of a reserve or volunteer in such a way that it would violate employment laws or labor agreements (e.g., a detention officer working as a reserve officer for reduced or no pay). Therefore, the Reserve Coordinator should consult the Department of Human Resources prior to an employee serving in a reserve or volunteer capacity (29 CFR 553.30).

324.3 DUTIES OF RESERVE AND AUXILIARY OFFICERS

Reserve officers assist regular officers in the enforcement of laws and in maintaining peace and order within the community. Assignments of reserve officers will usually be to augment the Patrol Division. Reserve officers may be assigned to other areas within the Department as needed. Reserve officers are required to work a minimum of 20 hours per month.

A reserve or auxiliary officer has peace officer authority only while engaged in the reserve or auxiliary activities authorized by the Chief of Police and shall only exercise that spectrum of peace officer authority that the Department is empowered to delegate and for which the officer has been trained and certified (Utah Code 53-13-111(1)(b)).

An auxiliary officer is limited to the role of backup to a law enforcement officer and may not initiate any action authorized for a law enforcement officer. An auxiliary officer may be separated from a law enforcement officer only under exigent circumstances or when engaged in functions not exclusive to law enforcement (Utah Code 53-13-112).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Reserve and Auxiliary Officers

An auxiliary officer may exercise that spectrum of peace officer authority that has been designated by statute to the Department, and only while on-duty, and not for the purpose of general law enforcement (Utah Code 53-13-105(2)(a)).

- (a) An auxiliary officer may not exercise the authority of a peace officer until the officer has satisfactorily completed an approved basic training program for special function officers and has been certified by the Chief of Police.

324.3.1 POLICY COMPLIANCE

Police reserve officers shall be required to adhere to every policy adopted by the Department. A copy of the Policy Manual will be made available to each reserve officer upon appointment and he/she shall become thoroughly familiar with these policies.

Whenever a rule, regulation or guideline in this manual refers to a sworn regular full-time officer, it shall also apply to a sworn reserve officer unless by its nature it is inapplicable.

324.3.2 RESERVE OFFICER ASSIGNMENTS

All reserve officers will be assigned to duties by the Reserve Coordinator or his/her designee.

324.3.3 RESERVE COORDINATOR

The Chief of Police shall delegate the responsibility for administering the Reserve Officer Program to a Reserve Coordinator.

The Reserve Coordinator shall have the responsibility of, but not be limited to:

- (a) Assignment of reserve personnel.
- (b) Conducting reserve meetings.
- (c) Establishing and maintaining a reserve callout roster.
- (d) Maintaining performance evaluations and ensuring they are completed.
- (e) Monitoring individual reserve officer performance.
- (f) Monitoring overall Reserve Program.
- (g) Maintaining liaison with other agency Reserve Coordinators.

324.4 FIELD TRAINING

The selection criteria for reserve officers shall be the same as for full time officers. Reserve officers must minimally be certifiable within the State of Utah as a Category II Peace Officer.

- (a) Reserve officers shall complete a recruit, or field training, program comparable to that of full time officers prior to any routine assignment in any capacity in which the reserve officer is allowed to carry a weapon or is in a position to make an arrest, except as part of a formal field-training program.
- (b) The training curriculum for reserve officers may be restricted to those specific functions they are authorized to perform.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Reserve and Auxiliary Officers

- (c) Uniforms and equipment for reserve officers shall be the same as required for full time officers performing like functions.
- (d) Reserve officers shall receive in-service training equivalent to that statutorily required for full time officers.
- (e) Reserve officers shall be trained in use of force policy, and tested for firearms proficiency with the same frequency of full time officers.
- (f) Reserve officers shall be provided with public liability protection equal to that of full time officers.
- (g) Reserve officers will abide by all department policies and procedures at all times.
- (h) Reserve officers wishing to ride for a tour of duty will coordinate with the Field Training Officer (FTO) they wish to ride with.
 - 1. Under no circumstances will a reserve officer appear for a ride-along without first coordinating with their FTO.
- (i) Once the reserve officer has completed the FTO program and has been released by the reserve officer sergeant, the reserve officer may only ride after first coordinating with the sergeant of the shift in question.
- (j) When reporting for duty, reserve officers will be in full police uniform, unless prior instructions have been given.
- (k) Reserve officers will follow all lawful orders and instructions of training personnel and full time officers.
- (l) Reserve officers shall be held to the same standards of conduct as full time officers.
- (m) Reserve officers shall have peace officer authority only while engaged in the activities authorized by the Chief of Police of the jurisdiction in which the officer serves.
- (n) Reserve officers may carry firearms only if authorized, and under conditions set forth by the Chief of Police.
- (o) Reserve officers shall not equip their personal vehicles with prohibited red lights or sirens, or any other device, which would lead a reasonable person to believe the vehicle or its occupant to be part of a police agency.
- (p) Reserve officers may not issue citations while off-duty, or engage in unauthorized outside employment requiring police uniforms or police powers.
- (q) Reserve officers are prohibited from carrying concealed weapons off-duty, unless otherwise authorized by law or the Chief of Police.
- (r) An identification card and badge and/or other such insignia or evidence of identification, shall be issued to each reserve officer, and shall be carried while on-duty. Reserve officer identification shall designate the officer's status as a reserve.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Reserve and Auxiliary Officers

- (s) It shall be unlawful for any person not a member of the South Salt Lake Police Department to wear, carry, or display a reserve identification card, badge, or insignia, or in any other manner represent his/herself to be connected to the South Salt Lake reserve program.
- (t) Under no circumstances shall a reserve officer be authorized to represent his/her status as that of a full time peace officer.
- (u) The Chief of Police, for cause satisfactory to his/herself may terminate the membership of any person in the reserve program at any time.
- (v) Any reserve officer may resign from the program at any time, upon notifying the department of such resignation.
- (w) Each reserve officer must surrender city-owned property upon termination of membership.
- (x) Reserve officers shall not work a tour of duty without being closely supervised by an FTO, unless otherwise directed by the Chief of Police or his/her designee.
 - 1. For the purpose of this subsection "designee's" are the Reserve Corps Sergeant, Division Commander and Deputy Chief of Police.

324.5 SUPERVISION OF RESERVE OFFICERS

Depending on their level of certification and number of hours with the [Department/Office], reserve officers who have attained the status of Level II shall be under the immediate supervision of a regular sworn officer.

Auxiliary officers shall work under the direction and immediate supervision of a certified law enforcement officer as defined in Utah Code 53-13-103.

324.5.1 RESERVE OFFICER MEETINGS

All reserve officer meetings will be scheduled and conducted by the Reserve Coordinator. All reserve officers are required to attend scheduled meetings. Any absences must be satisfactorily explained to the Reserve Coordinator.

324.5.2 IDENTIFICATION OF RESERVE OFFICERS

All reserve officers will be issued a uniform badge and a Department identification card. The uniform badge shall be the same as that worn by a regular full-time officer. The identification card will be the standard identification card with the exception that "Reserve" will be indicated on the card.

324.5.3 UNIFORM AND EQUIPMENT

The reserve officer uniform shall be the same as that worn by a regular full-time officer. Reserve officers shall conform to all uniform regulations and appearance standards of the [Department/Office].

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Reserve and Auxiliary Officers

All reserve officers shall have access to the same equipment as regular officers performing like functions.

324.5.4 INVESTIGATIONS AND COMPLAINTS

If a reserve officer has a complaint made against him/her or becomes involved in an internal investigation, that complaint or internal investigation may be investigated by the Reserve Coordinator, at the discretion of the Division Commanders.

Reserve officers are considered at-will employees.

Any disciplinary action that may have to be administered to a reserve officer shall be accomplished as outlined in the Policy Manual.

324.6 FIREARMS REQUIREMENTS

324.6.1 CARRYING WEAPON ON-DUTY

Reserve officers may carry a loaded firearm while on-duty. It is the policy of the Department to allow reserves to carry firearms only while on-duty or to and from duty.

Auxiliary officers may carry firearms only while on-duty, and only if authorized and under conditions specified by the Department (Utah Code 53-13-105(2)(c)).

324.6.2 ADDITIONAL CONSIDERATIONS

A reserve officer shall not carry a concealed [department/office] firearm while in an off-duty capacity, other than to and from work. A personally owned firearm may be carried off-duty only if the officer possesses a valid Concealed Weapon License (CWL) issued by the Department of Public Safety, Bureau of Criminal Investigation or is otherwise authorized under state law or the Law Enforcement Officers' Safety Act (18 USC § 926B).

An instance may arise where a reserve officer is assigned to a plainclothes detail for their assigned tour of duty. Under these circumstances, the officer may be permitted to carry a weapon more suited to the assignment with the knowledge and approval of the supervisor in charge of the detail.

Any reserve officer who is permitted to carry a firearm other than the assigned duty weapon may do so only after verifying that the weapon conforms to [department/office] standards. The weapon must be registered by the reserve officer and be inspected and certified as fit for service by a [department/office] armorer.

Before being allowed to carry any optional firearm during an assigned tour of duty the reserve officer shall have demonstrated their proficiency with said weapon.

324.6.3 RESERVE OFFICER FIREARM TRAINING

All reserve officers are required to maintain proficiency with firearms used in the course of their assignments. Reserve officers shall comply with all areas of the firearms training section of the Policy Manual, with the following exceptions:

- (a) All reserve officers are required to qualify at the same standards as a Full Time Officers

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Reserve and Auxiliary Officers

- (b) Should a reserve officer fail to qualify, that reserve officer will not be allowed to carry a firearm until proficiency has been reestablished.

324.7 EMERGENCY CALLOUT FOR RESERVE PERSONNEL

The Reserve Coordinator shall develop a plan outlining an emergency callout procedure for reserve personnel.

324.8 AUXILIARIES AND VOLUNTEERS

The South Salt Lake City Police Department Volunteer Unit will be comprised of highly motivated, civic and/or spiritually minded individuals who are called upon to give of their time and energy to support the mission of the department.

324.8.1 POLICY

- (a) The functions of the South Salt Lake City Police Department Volunteer program will include:
 - 1. Increasing the involvement of qualified citizens in the law enforcement mission.
 - 2. Providing police-related community services.
 - 3. Provide necessary services to employees of the department and/or their families in times of crisis.
 - 4. Providing a competent augmentation and assistance to the police department during times of emergencies, disasters, and special events through the deployment of volunteers.
- (b) Auxiliary/Volunteer Status
 - 1. Volunteers will not have the authority to make arrests, or be utilized for duties, which would require a sworn officer status.
 - 2. Under no circumstances is a volunteer to engage in a confrontation during their volunteer tour of duty time.
 - 3. If or when a confrontation occurs, the volunteer is directed to walk away and report the incident to their supervisor as soon as possible.
- (c) Duties of Auxiliary/Volunteers
 - 1. The South Salt Lake City Police volunteers shall function under the general direction of the Chief of Police or his/her designee and will be directly assigned, upon completion of training, to the volunteer coordinator, with the exception of the police chaplains.
 - (a) Volunteer chaplains will be utilized on an "as-needed" basis.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Reserve and Auxiliary Officers

- (b) Volunteer chaplains will be issued a badge and police identification, identifying them as a Police Chaplain of the South Salt Lake City Police Department.
 - (c) All issued identification will be returned to the department upon notification of separation from any position.
 - 2. Volunteers will be subject to the rules set forth in the city ordinances, police code of conduct, general orders, standard operating procedures, and other rules and regulations that may be set forth by the Chief of Police.
 - 3. The volunteer program will be administered and directed by the volunteer coordinator, who reports directly to the Crime Prevention sergeant.
 - 4. Volunteers will, in part, function in support of community relations activities and other civilian level support activities.
 - 5. The training of volunteers is a unique task. Therefore, each of the volunteer groups will be trained according to the duties they have agreed to perform. The training will be coordinated through the administrative sergeant and/or volunteer coordinator.
 - 6. Volunteers will not wear police uniforms but will be issued identification cards to identify their status with the department.
- (d) Volunteer's will be processed as follows, before receiving department identification or after notice of separation:
- (a) Completed applications will be submitted to the respective Division Commander, who will consult with the Chief of Police or his/her designee for approval to proceed with a background check. If the application is disapproved the applicant will be notified in writing.
 - (b) Personnel from the Investigations section will complete background checks.
 - (c) After the background is completed, the Division Commander will review the results.
 - (a) If the results are satisfactory, the applicant will be issued city and/or department identification indicating their Police volunteer status.
 - (b) If the results of the background are not satisfactory the applicant will be notified in writing, and be provided with the opportunity to provide explanation(s).
 - (c) The Chief of Police will have the final decision on this matter.
 - (d) The volunteer will then be assigned to a supervisor for training and deployment.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Reserve and Auxiliary Officers

- (e) At such time as the volunteer leaves the services of the department, the Crime Prevention sergeant will insure that the volunteer returns all issued equipment and identification.

324.9 LIABILITY PROTECTION

Reserve officers shall be provided liability protection in the same manner as regular officers performing like functions.

Outside Agency Assistance

325.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance to members when requesting or responding to a request for mutual aid or when assisting another law enforcement agency.

325.2 POLICY

It is the policy of the South Salt Lake Police Department to promptly respond to requests for assistance by other law enforcement agencies, subject to available resources and consistent with the applicable laws and policies of this department.

325.3 ASSISTING OUTSIDE AGENCIES

Generally, requests for any type of assistance from another agency should be routed to the Watch Commander's office for approval. In some instances, a mutual aid agreement or other established protocol may exist that eliminates the need for approval of individual requests.

When another law enforcement agency requests assistance from this department, the Watch Commander may authorize, if available, an appropriate number of personnel to assist. Members are reminded that their actions when rendering assistance must conform with applicable laws and be consistent with the policies of this department.

Officers may respond to a request for emergency assistance, however, they shall notify a supervisor of their activity as soon as practicable.

Arrestees may be temporarily detained by this department until arrangements for transportation are made by the outside agency. Probation violators who are temporarily detained by this department will not ordinarily be booked at this department. Only in exceptional circumstances, and subject to supervisor approval, will this department provide transportation of arrestees to other facilities on behalf of another agency.

When transportation assistance is rendered, a report shall be prepared and submitted by the handling member unless otherwise directed by a supervisor.

325.3.1 INITIATED ACTIVITY

Prior to an officer taking any action beyond the limits of the officer's normal jurisdiction, the officer shall notify and receive approval of the local law enforcement authority, or if the prior contact is not reasonably possible, notify the local law enforcement authority as soon as reasonably possible (Utah Code 77-9-3).

Any on-duty officer who engages in law enforcement activities of any type that are not part of a mutual aid request and take place outside the jurisdiction of the South Salt Lake Police Department shall notify his/her supervisor or the Watch Commander and Dispatch as soon as practicable. This requirement does not apply to special enforcement details or multi-agency units that regularly work in multiple jurisdictions.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Outside Agency Assistance

325.4 REQUESTING OUTSIDE ASSISTANCE

If assistance is needed from another agency, the member requesting assistance should, if practicable, first notify a supervisor. The handling member or supervisor should direct assisting personnel to where they are needed and to whom they should report when they arrive.

The requesting member should arrange for appropriate radio communication capabilities, if necessary and available, so that communication can be coordinated between assisting personnel.

325.5 REPORTING REQUIREMENTS

Incidents of outside assistance or law enforcement activities that are not documented in a crime report shall be documented in a general case report or as directed by the Watch Commander.

325.6 MANDATORY SHARING

Equipment and supplies purchased with federal funds or grants that require such equipment and supplies be shared with other agencies should be documented and updated as necessary by the Administration Division Commander or the authorized designee.

The documentation should include:

- (a) The conditions relative to sharing.
- (b) The training requirements for:
 - 1. The use of the supplies and equipment.
 - 2. The members trained in the use of the supplies and equipment.
- (c) Any other requirements for use of the equipment and supplies.

Copies of the documentation should be provided to Dispatch and the Watch Commander to ensure use of the equipment and supplies is in compliance with the applicable sharing agreements.

The Training Coordinator should maintain documentation that the appropriate members have received the required training.

Registered Offender Information

326.1 PURPOSE AND SCOPE

This policy establishes guidelines by which the South Salt Lake Police Department will address issues associated with certain offenders who are residing in the jurisdiction and how the [Department/Office] will disseminate information and respond to public inquiries for information about registered sex, kidnap, and child abuse offenders.

326.2 POLICY

It is the policy of the South Salt Lake Police Department to identify and monitor registered offenders living within this jurisdiction and to take reasonable steps to address the risks those persons may pose.

326.3 REGISTRATION

The Investigations Division supervisor shall establish a process to reasonably accommodate registration of certain offenders. The process should rebut any allegation on the part of the offender that the registration process was too confusing, burdensome, or difficult for compliance. If it is reasonable to do so, an investigator assigned to related investigations should conduct the registration in order to best evaluate any threat the person may pose to the community.

Upon conclusion of the registration process, the investigator shall ensure that the registration information is provided to the Utah Department of Public Safety (DPS).

The refusal of a registrant to provide any of the required information or complete the process should initiate a criminal investigation for failure to register (Utah Code 53-29-305).

326.3.1 CONTENTS OF REGISTRATION

Members assigned to register offenders should obtain the following information from registering offenders (Utah Code 53-29-304):

- (a) All names and aliases
- (b) The primary and secondary residence addresses
- (c) A physical description, date of birth, height, weight, eye, and hair color
- (d) The make, model, color, year, plate number, and vehicle identification number of any vehicle or vehicles owned or driven more than 12 times per year
- (e) A current photograph
- (f) A set of fingerprints, if one has not already been provided
- (g) A DNA specimen, taken in accordance with Utah Code 53-10-404, if one has not already been provided
- (h) Telephone numbers and any other designations used for routing or self-identification in telephonic communications from fixed locations or cellular telephones

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Registered Offender Information

- (i) Internet identifiers and any addresses used for routing or self-identification in internet communications or postings
- (j) The name and internet address of all websites on which the person is registered using an online identifier, including all online identifiers used to access those websites
- (k) A copy of any passport
- (l) If the person is an alien, all documents establishing immigration status
- (m) All professional licenses that authorize engaging in an occupation or carrying out a trade or business, including any identifiers, such as numbers
- (n) Each educational institution in Utah at which the person is employed, carries on a vocation, or is a student, and any change of enrollment or employment status at any educational institution
- (o) The name, telephone number, and address of any place of employment
- (p) The name, telephone number, and address of any place where the person volunteers
- (q) The person's Social Security number

Members assigned to register offenders should inform the offender of the duty to comply with the continuing registration requirements and identification card requirements, if applicable (Utah Code 53-29-302).

326.4 MONITORING OF REGISTERED OFFENDERS

The Investigations Division supervisor should establish a system to periodically, and at least once annually, verify that a registrant remains in compliance with registration requirements after the initial registration. This verification should include:

- (a) Efforts to confirm residence using an unobtrusive method, such as an internet search or drive-by of the declared residence.
- (b) Review of information on DPS's Sex, Kidnap, and Child Abuse Offender Notification and Registration (SONAR) website.
- (c) Contact with a registrant's parole or probation officer.

Any discrepancies should be reported to DPS.

The Investigations Division supervisor should also establish a procedure to routinely disseminate information regarding registered offenders to South Salt Lake Police Department personnel, including timely updates regarding new or relocated registrants.

326.5 DISSEMINATION OF PUBLIC INFORMATION

Members will not unilaterally make a public notification advising the community of a particular registrant's presence in the community. Members who identify a significant risk or other public safety issue associated with a registrant should promptly advise their supervisor. The supervisor should evaluate the request and forward the information to the Chief of Police if warranted. A determination will be made by the Chief of Police, with the assistance of legal counsel as necessary, whether such a public alert should be made.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Registered Offender Information

Members of the public requesting information on registrants should be directed to the DPS's SONAR website for specific registrant information and photographs (Utah Code 53-29-404).

The Records Supervisor shall release local registered offender information to residents in accordance with Utah Code 53-29-303 and in compliance with a Government Records Access and Management Act (GRAMA) request.

326.5.1 RELEASE NOTIFICATIONS

Registrant information that is released should include notification that:

- (a) The offender registry includes only those persons who have been required by law to register and who are in compliance with the offender registration laws.
- (b) The information is provided as a public service and may not be current or accurate.
- (c) Persons should not rely solely on the offender registry as a safeguard against offenses in their communities.
- (d) The crime for which a person is convicted may not accurately reflect the level of risk.
- (e) Anyone who uses information contained in the registry to harass registrants or commit any crime may be subject to criminal prosecution.

326.6 LEGAL MANDATES AND RELEVANT LAWS

Members responsible for registering and entering sex, kidnap, or child abuse offenders into the database must be certified by the Utah DPS. To obtain and retain certification, the employee must receive initial and annual training from DPS (Utah Code 53-29-302).

The Training Coordinator will be responsible for ensuring the appropriate training and certifications are maintained.

Major Incident Notification

327.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance to members of this department in determining when, how and to whom notification of major incidents should be made.

327.2 POLICY

The South Salt Lake Police Department recognizes that certain incidents should be brought to the attention of supervisors or other specified personnel of this department to facilitate the coordination of activities and ensure that inquiries from the media and the public may be properly addressed.

327.3 MINIMUM CRITERIA FOR NOTIFICATION

Most situations where the media shows a strong interest are also of interest to the Chief of Police and the affected Division Commander. The following list of incident types is provided as a guide for notification and is not intended to be all-inclusive:

- Unattended deaths or serious bodily injury
- Traffic accidents with fatalities
- Officer-involved shooting on- or off-duty (See the Officer-Involved Shootings and Deaths Policy for special notifications)
- Significant injury or death to employee on- or off-duty
- Death of a prominent South Salt Lake official
- Arrest of Department employee or prominent South Salt Lake official
- Aircraft crash with major damage and/or injury or death
- In-custody deaths
- AMBER or SILVER Alerts
- SWAT or POU Call Out
- Industrial accident with serious bodily injury or death
- Missing Endangered Juvenile
- Any incident where there is a media request or interest.
- Any evacuation support.
- Unified Command Incident
- Any other incident of concern.

327.4 WATCH COMMANDER RESPONSIBILITY

The Watch Commander is responsible for making the appropriate notifications. The Watch Commander shall make reasonable attempts to obtain as much information on the incident as possible before notification. The Watch Commander shall attempt to make the notifications as

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Major Incident Notification

soon as practical. Notification should be made by texting the administrative command staff group. If notification is not acknowledge, within 15 minutes, a phone call to your immediate supervisor should be made. If your immediate supervisor does not acknowledge within 15 minutes of a phone call, continue to make contact up the chain of command. Continual efforts should be made until contact is made with a member from the administrative command staff. Situational updates should be texted to the administrative command staff group as an incident evolves. There should be a final Significant Incident report submitted via email to the command staff, prior to going off shift. The Significant Incident Report should include incident information; case number, date, time, location of incident, type of incident, officers involved, injuries, summary of incident and what actions still need to be addressed.

327.4.1 STAFF NOTIFICATION

In the event an incident occurs described in MINIMUM CRITERIA FOR NOTIFICATION, the Chief of Police shall be notified along with the affected Division Commander and the Detective Lieutenant if that division is affected.

327.4.2 DETECTIVE NOTIFICATION

If the incident requires that a detective respond from home, the immediate supervisor of the appropriate detail shall be contacted who will then contact the appropriate detective. The Detective Lieutenant shall notify the Deputy Chief and Chief.

327.4.3 MAJOR ACCIDENT UNIT NOTIFICATION

In the event of a traffic fatality or major injury, the supervisor over the Major Accident Unit shall be notified who will then contact the appropriate accident investigator. The Major Accident Supervisor shall notify the Deputy Chief and Chief.

327.4.4 PUBLIC INFORMATION OFFICER

The Public Information Officer shall be called after members of Staff have been notified that it appears the media may have a significant interest in the incident.

Death Investigation

328.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for when officers initially respond to and investigate the circumstances of a deceased person. Investigations involving the death of a person, including those from natural causes, accidents, workplace incidents, suicide, in-custody death, and homicide, shall be initiated, conducted and properly documented. Some causes of death may not be readily apparent, and some cases differ substantially from what they appeared to be initially. Thorough death investigations and the use of appropriate resources and evidence-gathering techniques are critical.

328.2 INVESTIGATION CONSIDERATIONS

Emergency Medical Services shall be called in all suspected death cases unless death is obvious (e.g., decapitated, decomposed).

A supervisor shall be notified as soon as possible to assist and provide appropriate personnel and resources. The on-scene supervisor should determine whether follow-up investigation is required and notify the Investigation Division Commander as necessary. The Watch Commander will make notification to command staff in accordance with the Major Incident Notification Policy.

328.2.1 [MEDICALEXAMINER/JOP] REQUEST

Officers are not authorized to pronounce death unless they are also [MedicalExaminer/JOP]s, Deputy [MedicalExaminer/JOP]s, or appointed [MedicalExaminer/JOP] investigators. The [MedicalExaminer/JOP] shall be called in all sudden or unexpected deaths, or deaths due to other than natural causes. State law requires that the [MedicalExaminer/JOP] be notified in any of the following cases (Utah Code 26B-8-205; Utah Code 26B-8-206):

- (a) Unattended deaths wherein the deceased has not been attended by a physician in a professional capacity in the 365 days prior to death (Utah Code 26B-8-201).
- (b) Deaths by violence, gunshot, suicide, or accident.
- (c) Sudden death while in apparent good health.
- (d) Unattended deaths, except that an autopsy may only be performed in accordance with the provisions of Utah Code 26B-8-207.
- (e) The death is under suspicious or unusual circumstances.
- (f) The death results from poisoning or overdose of drugs.
- (g) The death results from diseases that may constitute a threat to the public health.
- (h) The death results from disease, injury, toxic effect, or unusual exertion incurred within the scope of the decedent's employment.
- (i) The death is due to sudden unexpected infant death.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Death Investigation

- (j) When a fetal death occurs without medical attendance at or immediately after the delivery or when inquiry is required by the Utah Medical Examiner Act (Utah Code 26B-8-115).
- (k) When there is a reason to believe that a child has died as a result of child abuse or neglect (Utah Code 80-2-604).
- (l) The death results while the decedent was in prison, jail, police custody, the state hospital, or in a detention or medical facility operated for the treatment of the mentally ill, emotionally disturbed, or delinquent persons.
- (m) The death is associated with diagnostic or therapeutic procedures.
- (n) When the death is being investigated as a homicide.
- (o) When a death results directly from the actions of a law enforcement officer.

328.2.2 SEARCHING DEAD BODIES

- (a) The [MedicalExaminer/JOP], the [MedicalExaminer/JOP]'s assistant, and authorized investigators are generally the only persons permitted to move, handle, or search a dead body.
- (b) An officer may make a reasonable search of an individual who it is reasonable to believe is dead, or near death, for the purpose of identification or for information identifying the individual as an anatomical donor. If a donor document is located, the [MedicalExaminer/JOP] or the [MedicalExaminer/JOP]'s assistant shall be promptly notified.
- (c) The [MedicalExaminer/JOP], with the permission of the [Department/Office], may take property, objects, or articles found on the deceased or in the immediate vicinity of the deceased that may be necessary for conducting an investigation to determine the identity of the deceased or the cause or manner of death.
- (d) Should exigent circumstances indicate to an officer that any other search of a known dead body is warranted prior to the arrival of the [MedicalExaminer/JOP] or the [MedicalExaminer/JOP]'s assistant, the investigating officer should first obtain verbal consent from the [MedicalExaminer/JOP] or the [MedicalExaminer/JOP]'s assistant when practicable.
- (e) Whenever reasonably possible, a witness, preferably a relative to the deceased or a member of the household, should be requested to remain nearby the scene and available to the officer pending the arrival of the [MedicalExaminer/JOP] or the [MedicalExaminer/JOP]'s assistant. The name and address of this person shall be included in the narrative of the death report.
- (f) Whenever personal effects are removed from the body of the deceased by the [MedicalExaminer/JOP] or the [MedicalExaminer/JOP]'s assistant, a receipt shall be obtained. This receipt shall be attached to the death report.

328.2.3 DEATH NOTIFICATION

When practicable, and if not handled by the Medical Examiner's Office, notification to the next-of-kin of the deceased person shall be made, in person, by the officer assigned to the incident. If

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Death Investigation

the next-of-kin lives in another jurisdiction, a law enforcement official from that jurisdiction shall be requested to make the personal notification. If the relatives live outside this county, the Medical Examiner may be requested to make the notification. The Medical Examiner needs to know if notification has been made. Assigned detectives may need to talk to the next-of-kin.

328.2.4 UNIDENTIFIED DEAD BODIES

If the identity of a dead body cannot be established, the Medical Examiner will assign a unique identifying number to the body and maintain a file under the assigned number. If possible, this number when applicable shall be included in any report.

328.2.5 DEATH INVESTIGATION REPORTING

All incidents involving a death shall be documented on the appropriate form.

328.2.6 SUSPECTED HOMICIDE

If the initially assigned officer suspects that the death involves a homicide or other suspicious circumstances, the officer shall take steps to protect the scene. The Investigations Division shall be notified to determine the possible need for an investigator to respond to the scene.

If the on-scene supervisor, through consultation with the Watch Commander or Investigations Division supervisor, is unable to determine the manner of death, the investigation shall proceed as though it is a homicide.

The investigator assigned to investigate a homicide or death that occurred under suspicious circumstances may, with the approval of his/her supervisor, request the Medical Examiner to conduct physical examinations and tests, and to provide a report.

328.2.7 EMPLOYMENT-RELATED DEATHS OR INJURIES

Any member of this agency who responds to and determines that a death, serious illness, or serious injury has occurred as a result of an accident at, or in connection with, the victim's employment, should ensure that the nearest office of the Utah Division of Occupational Safety and Health is notified with all pertinent information.

Limited English Proficiency Services

330.1 PURPOSE AND SCOPE

This policy provides guidance to members when communicating with individuals with limited English proficiency (LEP) (42 USC § 2000d).

330.1.1 DEFINITIONS

Definitions related to this policy include:

Authorized interpreter - A person who has been screened and authorized by the Department to act as an interpreter and/or translator for others.

Interpret or interpretation - The act of listening to a communication in one language (source language) and orally converting it to another language (target language), while retaining the same meaning.

Limited English proficient (LEP) - Any individual whose primary language is not English and who has a limited ability to read, write, speak or understand English. These individuals may be competent in certain types of communication (e.g., speaking or understanding) but still be LEP for other purposes (e.g., reading or writing). Similarly, LEP designations are context-specific; an individual may possess sufficient English language skills to function in one setting but these skills may be insufficient in other situations.

Qualified bilingual member - A member of the South Salt Lake Police Department, designated by the Department, who has the ability to communicate fluently, directly and accurately in both English and another language. Bilingual members may be fluent enough to communicate in a non-English language but may not be sufficiently fluent to interpret or translate from one language into another.

Translate or translation - The replacement of written text from one language (source language) into an equivalent written text (target language).

330.2 POLICY

It is the policy of the South Salt Lake Police Department to reasonably ensure that LEP individuals have meaningful access to law enforcement services, programs and activities, while not imposing undue burdens on its members.

The Department will not discriminate against or deny any individual access to services, rights or programs based upon national origin or any other protected interest or right.

330.3 LEP COORDINATOR

The Chief of Police shall delegate certain responsibilities to an LEP Coordinator. The LEP Coordinator shall be appointed by, and directly responsible to, the Patrol Division Commander or the authorized designee.

The responsibilities of the LEP Coordinator include, but are not limited to:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Limited English Proficiency Services

- (a) Coordinating and implementing all aspects of the South Salt Lake Police Department's LEP services to LEP individuals.
- (b) Developing procedures that will enable members to access LEP services, including telephonic interpreters, and ensuring the procedures are available to all members.
- (c) Ensuring that a list of all qualified bilingual members and authorized interpreters is maintained and available to each Watch Commander and Dispatch Supervisor. The list should include information regarding the following:
 - 1. Languages spoken
 - 2. Contact information
 - 3. Availability
- (d) Ensuring signage stating that interpreters are available free of charge to LEP individuals is posted in appropriate areas and in the most commonly spoken languages.
- (e) Reviewing existing and newly developed documents to determine which are vital documents and should be translated, and into which languages the documents should be translated.
- (f) Annually assessing demographic data and other resources, including contracted language services utilization data and community-based organizations, to determine if there are additional documents or languages that are appropriate for translation.
- (g) Identifying standards and assessments to be used by the Department to qualify individuals as qualified bilingual members or authorized interpreters.
- (h) Periodically reviewing efforts of the Department in providing meaningful access to LEP individuals, and, as appropriate, developing reports, new procedures or recommending modifications to this policy.
- (i) Receiving and responding to complaints regarding department LEP services.
- (j) Ensuring appropriate processes are in place to provide for the prompt and equitable resolution of complaints and inquiries regarding discrimination in access to department services, programs and activities.

330.4 FOUR-FACTOR ANALYSIS

Since there are many different languages that members could encounter, the Department will utilize the four-factor analysis outlined in the U.S. Department of Justice (DOJ) Guidance to Federal Financial Assistance Recipients, available at the DOJ website, to determine which measures will provide meaningful access to its services and programs. It is recognized that law enforcement contacts and circumstances will vary considerably. This analysis, therefore, must remain flexible and will require an ongoing balance of four factors, which are:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Limited English Proficiency Services

- (a) The number or proportion of LEP individuals eligible to be served or likely to be encountered by department members, or who may benefit from programs or services within the jurisdiction of the Department or a particular geographic area.
- (b) The frequency with which LEP individuals are likely to come in contact with department members, programs or services.
- (c) The nature and importance of the contact, program, information or service provided.
- (d) The cost of providing LEP assistance and the resources available.

330.5 TYPES OF LEP ASSISTANCE AVAILABLE

South Salt Lake Police Department members should never refuse service to an LEP individual who is requesting assistance, nor should they require an LEP individual to furnish an interpreter as a condition for receiving assistance. The Department will make every reasonable effort to provide meaningful and timely assistance to LEP individuals through a variety of services.

The Department will utilize all reasonably available tools, such as language identification cards, when attempting to determine an LEP individual's primary language.

LEP individuals may choose to accept department-provided LEP services at no cost or they may choose to provide their own.

Department-provided LEP services may include, but are not limited to, the assistance methods described in this policy.

330.6 WRITTEN FORMS AND GUIDELINES

Vital documents or those that are frequently used should be translated into languages most likely to be encountered. The LEP Coordinator will arrange to make these translated documents available to members and other appropriate individuals, as necessary.

330.7 AUDIO RECORDINGS

The Department may develop audio recordings of important or frequently requested information in a language most likely to be understood by those LEP individuals who are representative of the community being served.

330.8 QUALIFIED BILINGUAL MEMBERS

Bilingual members may be qualified to provide LEP services when they have demonstrated through established department procedures a sufficient level of skill and competence to fluently communicate in both English and a non-English language. Members utilized for LEP services must demonstrate knowledge of the functions of an interpreter/translator and the ethical issues involved when acting as a language conduit. Additionally, bilingual members must be able to communicate technical and law enforcement terminology, and be sufficiently proficient in the non-English language to perform complicated tasks, such as conducting interrogations, taking statements, collecting evidence or conveying rights or responsibilities.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Limited English Proficiency Services

When a qualified bilingual member from this department is not available, personnel from other City departments, who have been identified by the Department as having the requisite skills and competence, may be requested.

330.9 AUTHORIZED INTERPRETERS

Any person designated by the Department to act as an authorized interpreter and/or translator must have demonstrated competence in both English and the involved non-English language, must have an understanding of the functions of an interpreter that allows for correct and effective translation, and should not be a person with an interest in the department case or investigation involving the LEP individual. A person providing interpretation or translation services may be required to establish the accuracy and trustworthiness of the interpretation or translation in a court proceeding.

Authorized interpreters must pass a screening process established by the LEP Coordinator which demonstrates that their skills and abilities include:

- (a) The competence and ability to communicate information accurately in both English and in the target language.
- (b) Knowledge, in both languages, of any specialized terms or concepts peculiar to this department and of any particularized vocabulary or phraseology used by the LEP individual.
- (c) The ability to understand and adhere to the interpreter role without deviating into other roles, such as counselor or legal adviser.
- (d) Knowledge of the ethical issues involved when acting as a language conduit.

330.9.1 SOURCES OF AUTHORIZED INTERPRETERS

The Department may contract with authorized interpreters who are available over the telephone. Members may use these services with the approval of a supervisor and in compliance with established procedures.

Other sources may include:

- Qualified bilingual members of this department or personnel from other City departments.
- Individuals employed exclusively to perform interpretation services.
- Contracted in-person interpreters, such as state or federal court interpreters, among others.
- Interpreters from other agencies who have been qualified as interpreters by this department, and with whom the Department has a resource-sharing or other arrangement that they will interpret according to department guidelines.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Limited English Proficiency Services

330.9.2 COMMUNITY VOLUNTEERS AND OTHER SOURCES OF LANGUAGE ASSISTANCE

Language assistance may be available from community volunteers who have demonstrated competence in either monolingual (direct) communication and/or in interpretation or translation (as noted in above), and have been approved by the Department to communicate with LEP individuals.

Where qualified bilingual members or other authorized interpreters are unavailable to assist, approved community volunteers who have demonstrated competence may be called upon when appropriate. However, department members must carefully consider the nature of the contact and the relationship between the LEP individual and the volunteer to ensure that the volunteer can provide neutral and unbiased assistance.

While family or friends of an LEP individual may offer to assist with communication or interpretation, members should carefully consider the circumstances before relying on such individuals. For example, children should not be relied upon except in exigent or very informal and non-confrontational situations.

330.10 CONTACT AND REPORTING

While all law enforcement contacts, services and individual rights are important, this department will utilize the four-factor analysis to prioritize service to LEP individuals so that such services may be targeted where they are most needed, according to the nature and importance of the particular law enforcement activity involved.

Whenever any member of this department is required to complete a report or other documentation and interpretation services are provided to any involved LEP individual, such services should be noted in the related report. Members should document the type of interpretation services utilized and whether the individual elected to use services provided by the Department or some other identified source.

330.11 RECEIVING AND RESPONDING TO REQUESTS FOR ASSISTANCE

The South Salt Lake Police Department will take reasonable steps and will work with the Department of Human Resources to develop in-house language capacity by hiring or appointing qualified members proficient in languages representative of the community being served.

330.11.1 EMERGENCY CALLS TO 9-1-1

Department members will make every reasonable effort to promptly accommodate LEP individuals utilizing 9-1-1 lines. When a 9-1-1 call-taker receives a call and determines that the caller is an LEP individual, the call-taker shall quickly determine whether sufficient information can be obtained to initiate an appropriate emergency response. If language assistance is still needed, the language is known and a qualified bilingual member is available in Dispatch, the call shall immediately be handled by the qualified bilingual member.

If a qualified bilingual member is not available or the call-taker is unable to identify the caller's language, the call-taker will contact the contracted telephone interpretation service and establish a three-way call between the call-taker, the LEP individual and the interpreter.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Limited English Proficiency Services

Dispatchers will make every reasonable effort to dispatch a qualified bilingual member to the assignment, if available and appropriate.

While 9-1-1 calls shall receive top priority, reasonable efforts should also be made to accommodate LEP individuals seeking routine access to services and information by utilizing the resources listed in this policy.

330.12 FIELD ENFORCEMENT

Field enforcement will generally include such contacts as traffic stops, pedestrian stops, serving warrants and restraining orders, crowd/traffic control and other routine field contacts that may involve LEP individuals. The scope and nature of these activities and contacts will inevitably vary. Members and/or supervisors must assess each situation to determine the need and availability of language assistance to all involved LEP individuals and utilize the methods outlined in this policy to provide such assistance.

Although not every situation can be addressed in this policy, it is important that members are able to effectively communicate the reason for a contact, the need for information and the meaning or consequences of any enforcement action. For example, it would be meaningless to request consent to search if the officer is unable to effectively communicate with an LEP individual.

If available, officers should obtain the assistance of a qualified bilingual member or an authorized interpreter before placing an LEP individual under arrest.

330.13 INVESTIGATIVE FIELD INTERVIEWS

In any situation where an interview may reveal information that could be used as the basis for arrest or prosecution of an LEP individual and a qualified bilingual member is unavailable or lacks the skills to directly communicate with the LEP individual, an authorized interpreter should be used. This includes interviews conducted during an investigation with victims, witnesses and suspects. In such situations, audio recordings of the interviews should be made when reasonably possible. Identification and contact information for the interpreter (e.g., name, address) should be documented so that the person can be subpoenaed for trial if necessary.

If an authorized interpreter is needed, officers should consider calling for an authorized interpreter in the following order:

- An authorized department member or allied agency interpreter
- An authorized telephone interpreter
- Any other authorized interpreter

Any *Miranda* warnings shall be provided to suspects in their primary language by an authorized interpreter or, if the suspect is literate, by providing a translated *Miranda* warning card.

The use of an LEP individual's bilingual friends, family members, children, neighbors or bystanders may be used only when a qualified bilingual member or authorized interpreter is unavailable and there is an immediate need to interview an LEP individual.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Limited English Proficiency Services

330.14 CUSTODIAL INTERROGATIONS

Miscommunication during custodial interrogations may have a substantial impact on the evidence presented in a criminal prosecution. Only qualified bilingual members or, if none is available or appropriate, authorized interpreters shall be used during custodial interrogations. *Miranda* warnings shall be provided to suspects in their primary language by the qualified bilingual member or an authorized interpreter.

In order to ensure that translations during custodial interrogations are accurately documented and are admissible as evidence, interrogations should be recorded whenever reasonably possible. See guidance on recording custodial interrogations in the Investigation and Prosecution Policy.

330.15 BOOKINGS

When gathering information during the booking process, members should remain alert to the impediments that language barriers can create. In the interest of the arrestee's health and welfare, the safety and security of the facility, and to protect individual rights, it is important that accurate medical screening and booking information be obtained. Members should seek the assistance of a qualified bilingual member whenever there is concern that accurate information cannot be obtained or that booking instructions may not be properly understood by an LEP individual.

330.16 COMPLAINTS

The Department shall ensure that LEP individuals who wish to file a complaint regarding members of this department are able to do so. The Department may provide an authorized interpreter or translated forms, as appropriate. Complaints will be referred to the LEP Coordinator.

Investigations into such complaints shall be handled in accordance with the Personnel Complaints Policy. Authorized interpreters used for any interview with an LEP individual during an investigation should not be members of this department.

Any notice required to be sent to an LEP individual as a complaining party pursuant to the Personnel Complaints Policy should be translated or otherwise communicated in a language-accessible manner.

330.17 COMMUNITY OUTREACH

Community outreach programs and other such services offered by this department are important to the ultimate success of more traditional law enforcement duties. This department will continue to work with community groups, local businesses and neighborhoods to provide equal access to such programs and services.

330.18 TRAINING

To ensure that all members who may have contact with LEP individuals are properly trained; the Department will provide periodic training on this policy and related procedures, including how to access department-authorized telephonic and in-person interpreters and other available resources.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Limited English Proficiency Services

The Training Coordinator shall be responsible for ensuring new members receive LEP training. Those who may have contact with LEP individuals should receive refresher training at least once every two years thereafter. The Training Coordinator shall maintain records of all LEP training provided, and will retain a copy in each member's training file in accordance with established records retention schedules.

330.18.1 TRAINING FOR AUTHORIZED INTERPRETERS

All members on the authorized interpreter list must successfully complete prescribed interpreter training. To complete interpreter training successfully, an interpreter must demonstrate proficiency in and ability to communicate information accurately in both English and in the target language, demonstrate knowledge in both languages of any specialized terms or phraseology, and understand and adhere to the interpreter role without deviating into other roles, such as counselor or legal adviser.

Members on the authorized interpreter list must receive refresher training annually or they will be removed from the authorized interpreter list. This annual training should include language skills competency (including specialized terminology) and ethical considerations.

The Training Coordinator shall be responsible for coordinating the annual refresher training and will maintain a record of all training the interpreters have received.

Mandatory Employer Notification

332.1 PURPOSE AND SCOPE

The purpose of this policy is to describe the notification requirements and procedures to follow when a school employee has been arrested for certain offenses.

332.2 POLICY

The South Salt Lake Police Department will meet the reporting mandates of Utah Code 53-10-211 to minimize the risks to children or others.

332.3 MANDATORY NOTIFICATION

If a school employee is arrested, or the Department receives information from another jurisdiction of a school employee's arrest, for any of the following offenses, the Chief of Police or the authorized designee shall immediately report the arrest to the State Board of Education and the superintendent of the school district that employs the employee (Utah Code 53-10-211):

- (a) Any controlled substance offense under Utah Code 58-37-8
- (b) Any offense under Utah Code 76-5-401 et seq. (sexual offenses)
- (c) Any offense involving sexual conduct

If the person is an employee of a private school, notification shall be made to the administrator of the school.

Public Safety Video Surveillance System

334.1 PURPOSE AND SCOPE

This policy provides guidance for the placement and monitoring of department public safety video surveillance, as well as the storage and release of the captured images.

This policy only applies to overt, marked public safety video surveillance systems operated by the Department. It does not apply to mobile audio/video systems, covert audio/video systems or any other image-capturing devices used by the Department.

334.2 POLICY

The South Salt Lake Police Department operates a public safety video surveillance system to complement its anti-crime strategy, to effectively allocate and deploy personnel, and to enhance public safety and security in public areas. Cameras may be placed in strategic locations throughout the City to detect and deter crime, to help safeguard against potential threats to the public, to help manage emergency response situations during natural and man-made disasters and to assist City officials in providing services to the community.

Video surveillance in public areas will be conducted in a legal and ethical manner while recognizing and protecting constitutional standards of privacy.

334.3 OPERATIONAL GUIDELINES

Only department-approved video surveillance equipment shall be utilized. Members authorized to monitor video surveillance equipment should only monitor public areas and public activities where no reasonable expectation of privacy exists. The Chief of Police or the authorized designee shall approve all proposed locations for the use of video surveillance technology and should consult with and be guided by legal counsel as necessary in making such determinations.

334.3.1 MONITORING

Camera placement will be guided by the underlying purpose or strategy associated with the overall video surveillance plan. As appropriate, the Chief of Police should confer with other affected City divisions and designated community groups when evaluating camera placement. Environmental factors, including lighting, location of buildings, presence of vegetation or other obstructions, should also be evaluated when determining placement.

Cameras shall only record video images and not sound. Recorded images may be used for a variety of purposes, including criminal investigations and monitoring of activity around high-value or high-threat areas. The public safety video surveillance system may be useful for the following purposes:

- (a) To prevent, deter and identify criminal activity.
- (b) To target identified areas of gang and narcotics complaints or activity.
- (c) To respond to critical incidents.
- (d) To assist in identifying, apprehending and prosecuting offenders.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Public Safety Video Surveillance System

- (e) To document officer and offender conduct during interactions to safeguard the rights of the public and officers.
- (f) To augment resources in a cost-effective manner.
- (g) To monitor pedestrian and vehicle traffic activity.

Images from each camera should be recorded in a manner consistent with the underlying purpose of the particular camera. Images should be transmitted to monitors installed in the Watch Commander's office and Dispatch. When activity warranting further investigation is reported or detected at any camera location, the available information should be provided to responding officers in a timely manner. The Watch Commander or trained personnel at Dispatch are authorized to adjust the cameras to more effectively view a particular area for any legitimate public safety purpose.

The Chief of Police may authorize video feeds from the public safety video surveillance system to be forwarded to a specified location for monitoring by other than police personnel, such as allied government agencies, road or traffic crews, or fire or emergency operations personnel.

Unauthorized recording, viewing, reproduction, dissemination or retention is prohibited.

334.3.2 CAMERA MARKINGS

All public areas that are monitored by public safety surveillance equipment shall be marked in a conspicuous manner with appropriate signs to inform the public that the area is under police surveillance. Signs should be well lit, placed appropriately and without obstruction to ensure visibility.

334.3.3 INTEGRATION WITH OTHER TECHNOLOGY

The Department may elect to integrate its public safety video surveillance system with other technology to enhance available information. Systems such as gunshot detection, incident mapping, crime analysis, license plate recognition, facial recognition and other video-based analytical systems may be considered based upon availability and the nature of department strategy.

The Department should evaluate the availability and propriety of networking or otherwise collaborating with appropriate private sector entities and should evaluate whether the use of certain camera systems, such as pan-tilt-zoom systems and video enhancement or other analytical technology, requires additional safeguards.

334.4 STORAGE AND RETENTION OF MEDIA

All downloaded media shall be stored in a secure area with access restricted to authorized persons. A recording needed as evidence shall be copied to a suitable medium and booked into evidence in accordance with established evidence procedures. All actions taken with respect to retention of media shall be appropriately documented.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Public Safety Video Surveillance System

The type of video surveillance technology employed and the manner in which recordings are used and stored will affect retention periods. The recordings should be stored and retained in accordance with the established records retention schedule.

334.4.1 EVIDENTIARY INTEGRITY

All downloaded and retained media shall be treated in the same manner as other evidence. Media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, digital masking of innocent or uninvolved individuals to preserve anonymity, authenticity certificates and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

334.5 RELEASE OF VIDEO IMAGES

All recorded video images gathered by the public safety video surveillance equipment are for the official use of the South Salt Lake Police Department.

Requests for recorded video images from the public or the media shall be processed in the same manner as requests for department public records.

Requests for recorded images from other law enforcement agencies shall be referred to the Watch Commander for release in accordance with a specific and legitimate law enforcement purpose.

Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

334.6 VIDEO SURVEILLANCE AUDIT

The Chief of Police or the authorized designee will conduct an annual review of the public safety video surveillance system. The review should include an analysis of the cost, benefit and effectiveness of the system, including any public safety issues that were effectively addressed or any significant prosecutions that resulted, and any systemic operational or administrative issues that were identified, including those related to training, discipline or policy.

The results of each review shall be appropriately documented and maintained by the Chief of Police or the authorized designee and other applicable advisory bodies. Any recommendations for training or policy should be promptly addressed.

334.7 VIDEO SUPERVISION

Supervisors should monitor video surveillance access and usage to ensure members are within department policy and applicable laws. Supervisors should ensure such use and access is appropriately documented.

334.7.1 VIDEO LOG

A log should be maintained at all locations where video surveillance monitors are located. The log should be used to document all persons not assigned to the monitoring locations who have

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Public Safety Video Surveillance System

been given access to view or monitor images provided by the video surveillance cameras. The logs should, at a minimum, record the:

- (a) Date and time access was given.
- (b) Name and agency of the person being given access to the images.
- (c) Name of person authorizing access.
- (d) Identifiable portion of images viewed.

334.7.2 PROHIBITED ACTIVITY

Public safety video surveillance systems will not intentionally be used to invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.

Public safety video surveillance equipment shall not be used in an unequal or discriminatory manner and shall not target individuals or groups based solely on actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability.

Video surveillance equipment shall not be used to harass, intimidate, or discriminate against any individual or group.

334.8 TRAINING

All department members authorized to operate or access public video surveillance systems shall receive appropriate training. Training should include guidance on the use of cameras, interaction with dispatch and patrol operations and a review regarding relevant policies and procedures, including this policy. Training should also address state and federal law related to the use of video surveillance equipment and privacy.

Unmanned Aerial System

335.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the use of an unmanned aerial system (UAS) and for the storage, retrieval, and dissemination of images and data captured by the UAS.

335.1.1 DEFINITIONS

Definitions related to this policy include:

Unmanned aerial system (UAS) - An unmanned aircraft of any type that is capable of sustaining flight, whether preprogrammed or remotely controlled (commonly referred to as an unmanned aerial vehicle (UAV)), and all of the supporting or attached systems designed for gathering information through imaging, recording, or any other means.

335.2 POLICY

A UAS may be utilized to enhance the department's mission of protecting lives and property when other means and resources are not available or are less effective. Any use of a UAS will be in strict accordance with constitutional and privacy rights and Federal Aviation Administration (FAA) regulations.

335.3 PRIVACY

The use of the UAS potentially involves privacy considerations. Absent a warrant or exigent circumstances, operators and observers shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure). Operators and observers shall take reasonable precautions to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy. Reasonable precautions can include, for example, deactivating or turning imaging devices away from such areas or persons during UAS operations.

335.4 PROGRAM COORDINATOR

The Chief of Police will appoint a program coordinator who will be responsible for the management of the UAS program. The program coordinator will ensure that policies and procedures conform to current laws, regulations, and best practices and will have the following additional responsibilities:

- Coordinating the FAA Certificate of Waiver or Authorization (COA) application process and ensuring that the COA is current, and/or coordinating compliance with FAA Part 107 Remote Pilot Certificate, as appropriate for [department/office] operations.
- Ensuring that all authorized operators and required observers have completed all required FAA and [department/office]-approved training in the operation, applicable laws, policies, and procedures regarding use of the UAS.
- Developing uniform protocols for submission and evaluation of requests to deploy a UAS, including urgent requests made during ongoing or emerging incidents. Deployment of a UAS shall require written authorization of the Chief of Police or the authorized designee, depending on the type of mission.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Unmanned Aerial System

- Coordinating the completion of the FAA Emergency Operation Request Form in emergency situations, as applicable (e.g., natural disasters, search and rescue, emergency situations to safeguard human life).
- Developing protocols for conducting criminal investigations involving a UAS, including documentation of time spent monitoring a subject.
- Implementing a system for public notification of UAS deployment.
- Developing operational protocols governing the deployment and operation of a UAS including but not limited to safety oversight, use of visual observers, establishment of lost link procedures, and secure communication with air traffic control facilities.
- Developing a protocol for fully documenting all missions.
- Developing UAS inspection, maintenance, and record-keeping protocol to ensure continuing airworthiness of a UAS, up to and including its overhaul or life limits.
- Developing protocols to ensure that all data intended to be used as evidence are accessed, maintained, stored, and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, authenticity certificates, and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.
- Facilitating law enforcement access to images and data captured by its UAS.
- Developing protocols that ensure retention and purge periods are maintained in accordance with established records retention schedules.
- Recommending program enhancements, particularly regarding safety and information security.
- Ensuring that established protocols are followed by monitoring and providing periodic reports on the program to the Chief of Police.
- Ensuring that data collected on a person, object, structure, or area that is not a target, as defined by Utah Code 72-10-801, is not used, copied, or disclosed except as allowed by law (Utah Code 72-10-803).
- Maintaining familiarity with FAA regulatory standards, state laws and regulations, and local ordinances regarding the operations of a UAS.

335.5 USE OF UAS

Only authorized operators who have completed the required training shall be permitted to operate the UAS.

Use of vision enhancement technology (e.g., thermal and other imaging equipment not generally available to the public) is permissible in viewing areas only where there is no protectable privacy interest or when in compliance with a search warrant or court order. In all other instances, legal counsel should be consulted.

UAS operations should only be conducted consistent with FAA regulations.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Unmanned Aerial System

Members shall not obtain, receive, or use data acquired through an UAS unless the data was obtained pursuant to a search warrant, obtained under a valid warrant exception, or used to locate a lost or missing person in an area where no person would have a reasonable expectation of privacy (Utah Code 72-10-802).

335.5.1 DATA COLLECTED BY PRIVATE CITIZEN

The South Salt Lake Police Department may not accept or review data captured by a privately-owned UAS unless one of the following conditions exists (Utah Code 72-10-802):

- (a) The person delivering the UAS data informs the [Department/Office] that the data appear to pertain to the commission of a crime.
- (b) The receiving member, in good faith, believes that the data pertain to an imminent or ongoing emergency that involves the danger of death or serious bodily injury to another person and that the disclosure of the data will permit the [Department/Office] to assist in responding to the emergency.

335.5.2 DOCUMENTATION

The following information must be documented in any related report or other record of the law enforcement encounter when the UAS is operated by a member of the South Salt Lake Police Department, or when the [Department/Office] obtains or receives data pursuant to Utah Code 72-10-802 (Utah Code 72-10-804):

- (a) The presence and use of the UAS
- (b) Any data acquired
- (c) If applicable, the private citizen from whom the data was received

335.5.3 TEMPORARY FLIGHT RESTRICTION DUE TO WILDLAND FIRES

A department UAS shall not be used in an area under a temporary flight restriction as a result of a wildland fire without the permission of, and in accordance with the restrictions established by, the official in command of the fire response (Utah Code 65A-3-2.5).

335.6 PROHIBITED USE

The UAS video surveillance equipment shall not be used:

- To conduct random surveillance activities.
- To target a person based solely on actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity, or expression, economic status, age, cultural group, or disability.
- To harass, intimidate, or discriminate against any individual or group.
- To conduct personal business of any type.

The UAS shall not be weaponized (Utah Code 72-10-902).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Unmanned Aerial System

335.7 RETENTION OF UAS DATA

The Records Section supervisor shall ensure that data collected by the UAS is deleted as soon as reasonably possible subject to applicable retention schedules under the Utah Government Records Access and Management Act (GRAMA) or a federal, state, or local law (Utah Code 72-10-802; Utah Code 72-10-803).

Communications to and from Field Officers

336.1 PURPOSE AND SCOPE

Valley Emergency Communications Center (VECC) will record the status of officers when they are on duty. Such records will allow the South Salt Lake City Police Department to evaluate non-patrol time for agency planning purposes, maintain a level of safety for the officers, and retain records of vehicles and persons stopped by officers.

(a) Radio procedures:

1. To ensure that all patrol officers and the communications center are aware of all units, the radio may be utilized for all instances of calling in and out of service, unless on specialized assignments.
2. Personnel may waive the requirements noted above with approval of a supervisor, if the nature of their activities dictates restrictions on the release of pertinent investigative information.
3. Patrol officers shall not be considered in or out of service until an acknowledgment is received from the dispatcher.
4. Patrol officers, when calling out of service, for any reason, shall give the location of the call-out and the reason for it, unless on specialized assignment.
5. Patrol officers assigned to radio equipped units, and when applicable, shall take their portable radios with them when they leave their vehicles for the purpose of maintaining contact with Dispatch.
6. Patrol officers shall, when calling the dispatcher, use their assigned radio call number and receive clearance, prior to transmitting any message other than a call for help or other emergency situation.
7. When called, patrol officers shall give their radio call number.
8. Each patrol officer shall respond to on-sight activity without delay, and at his/her convenience, notify the dispatcher of such action so that an incident can be prepared on such activity according to procedure.
 - (a) Notification before leaving the vehicle is preferred provided it does not affect the officer's safety or efficiency.
9. Each patrol officer shall respond to radio dispatched calls for service by giving his/her radio call number, location and acknowledge he/she has received the assignment.
 - (a) Each patrol officer shall inform dispatch of his/her arrival at the scene of radio dispatched calls, and inform dispatch that he/she is clearing the scene.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Communications to and from Field Officers

10. Radio traffic between units should be held to a minimum and should be allowed under the following circumstances:
 - (a) An interchange of information between units is necessary to accomplish a police objective.
 - (b) Several items of information must be exchanged between the units, and it would be impractical for the dispatcher to relay the information or for the units to meet and exchange the information.
 - (c) Officers should not leave their assigned communities or go to cover calls unless directed to do so by a supervisor.
11. To aid in keeping the air clear for emergencies and for dispatching calls, the telephone will be used for the purposes of:
 - (a) Providing the communications center with lengthy descriptions and details intended for broadcast to all units.
 1. If this is not practical and time is of the essence, the officer may transmit such information.
 - (b) Providing the communications center with pertinent information relating to the availability of staffing, special assignments, etc., by supervisory personnel.
 - (c) In the event of radio failure, the communications center should be so advised by telephone.
12. Radio interaction with outside/allied agencies:
 - (a) If officers need to communicate with outside agencies, they will switch their radios to the statewide channel or the other agency's channel.
 - (b) If the outside agency shares the South Salt Lake radio channel, officers may ask the other agency personnel to switch to an alternate channel for their conversations.
13. Officers shall not make inquiry of a dispatcher for specific ordinance sections to cover violations. Officers are expected to have this information with them, when on duty.
14. Officers in the field should refrain from having dispatch make personal phone calls for them except when it is absolutely necessary.
15. Officers who are out-of-service for any reason at the end of their tour-of-duty shall return in-service via radio before going off-duty.
16. Officer(s) will be responsible for handling assigned incidents and for informing the supervisor of the progress toward resolution (Except as noted in b.5 below.)

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Communications to and from Field Officers

17. Officer(s) shall communicate via radio with dispatch when they are transporting a prisoner of the opposite sex, or providing a shuttle for an individual of the opposite sex, by providing their beginning mileage prior to transporting and their ending mileage once they have reached their desired destination.
 - (a) If equipped with a Mobile Audio Video (MAV) system, the officer(s) shall activate the recording devices when they are transporting a prisoner of the opposite sex, or providing a shuttle for an individual of the opposite sex.
- (b) Supervisor Responsibilities:
 1. The on-duty shift supervisor will ensure that he/she remains in radio contact with Dispatch at all times. In the event he/she may be out of radio contact, he/she should provide a phone number where he/she may be contacted.
 2. Shift supervisors will confirm with Dispatch at the beginning of a shift, those officers who are on-duty, including specific assignments.
 3. It is the duty of a shift supervisor to provide the necessary command presence to facilitate the proper completion of an incident or crime investigation.
 4. A shift supervisor should respond to the following incidents:
 - (a) Most major in-progress calls involving threat of physical violence, injury, trauma, use of a deadly weapon, or substantial property loss.
 - (b) Child abuse.
 - (c) Kidnappings.
 - (d) Aggravated assaults involving critical injuries.
 - (e) Accidents that result in serious injury, death, or involve a city owned vehicle.
 - (f) Most incidents involving the execution of a consent search or search warrant.
 - (g) Any incident that a supervisor deems his/her presence may be required.
 5. Shift supervisors will respond to take command of and be responsible for coordination of the following incidents:
 - (a) Officer involved shooting.
 - (b) Barricaded or hostage situations.
 - (c) Traffic accidents involving on-duty police personnel.
 - (d) Dead body calls.
 - (e) Incidents involving injury to officers.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Communications to and from Field Officers

6. The shift supervisor will monitor the activities of the assigned officers and ensure all actions by officers are in compliance with departmental directives and the law.
 - (a) If the actions of the assigned officer are inappropriate, the shift supervisor may advise, counsel, or relieve the affected officer.
 - (b) The shift supervisor may relieve the assigned officer in command of the scene.
 - (c) Once the supervisor relieves the officer in command of an incident or investigation, the supervisor then assumes command of that specific incident.

Youth Resource Officer Program

337.1 PURPOSE AND SCOPE

The South Salt Lake Police Department is committed to safety in South Salt Lake City schools and therefore stations officer(s) within the schools to act as liaisons, additional resources, and delinquency and truancy prevention. The officer also provides an ethical example to the students both in the classroom and as a mentor. The officer also explains the role of policing and law enforcement in the community as well as in the school setting.

337.1.1 POLICY

- (a) Officers selected for the youth resource officer position must be able to further the departmental goals by adhering to this policy as well as adhering to the community policing philosophy. In addition the youth resource officer must do the following:
 - 1. Establish and build trust with the parents, students, faculty and citizens (especially those citizens living around and near the schools).
 - 2. Establish and maintain a positive, professional working relationship with the Granite School District Police, Promise SSL, and SSL Police Athletic League (PAL) as well as the juvenile courts.
 - 3. Build effective relationships, and demonstrate a genuine desire to succeed.
 - 4. Have an interest in students and in shaping the community's future.
 - 5. Mentor students dealing with personal issues through one-on-one discussions or with a school administrator present.
 - 6. Make visits to students' homes to discuss excessive absences, as well as enforcing truancy laws.
 - 7. Properly teach law enforcement vocational classes, including the development of a class syllabus, and the development and administration of required tests (High School SRO).
- (b) The Youth Resource Officer is the primary liaison with Granite School District, Promise SSL and SSL Police Athletic League to ensure timely coordination, planning of school safety protocol measures and activities. To include but not limited to after-school programming, monthly Bowl with a Cop, Youth Summer Camp (2 weeks annually budget dependent) and working with schools within South Salt Lake City on safety planning and addressing all requirements per Utah State Law.
- (c) Officer(s) will be stationed at the school for the duration of the school day, unless performing home visits or other school-related activities.
- (d) Youth Resource Officers are not intended for use as a security guards, but are stationed at schools to assist with the enforcement of school rules, maintain order and safety, and to enforce Utah laws.
- (e) When school is not in session, youth resource officers are expected to plan for the next school year, taking into consideration issues arising in the previous school year.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Youth Resource Officer Program

1. The officer will also develop lesson plans, investigate and resolve assigned juvenile cases, and develop NOVA lessons and crime prevention curriculum if appropriate.
 2. During the time that school is not in session, the officer may be re-assigned to other duties as deemed necessary by the Division Commanders or his/her designee.
- (f) Youth Resource Officers should always be cognizant of juvenile programs in the community, including mental health programs, drug abuse programs, youth recreational programs and anti-gang programs.
- (g) The position of Youth Resource Officer is designated as a specialty assignment. Officer's are chosen via a selection process for this position.

337.1.2 YOUTH RESOURCE OFFICER POSITION ANNUAL REVIEW

The YouthResource Officer position is based on the approval by the Chief of Police, budget constraints, and school district funding. All of these issues will be taken into consideration to determine whether or not the position will be filled.

Child and Dependent Adult Safety

338.1 PURPOSE AND SCOPE

This policy provides guidelines to ensure that children and dependent adults are not left without appropriate care in the event their caregiver or guardian is arrested or otherwise prevented from providing care due to actions taken by members of this department.

This policy does not address the actions to be taken during the course of a child abuse or dependent adult investigation. These are covered in the Child Abuse Policy and the Adult Abuse Policy.

338.2 POLICY

It is the policy of this department to mitigate, to the extent reasonably possible, the stressful experience individuals may have when their parent or caregiver is arrested. The South Salt Lake Police Department will endeavor to create a strong, cooperative relationship with local, state and community-based social services to ensure an effective, collaborative response that addresses the needs of those affected, including call-out availability and follow-up responsibilities.

338.3 PROCEDURES DURING AN ARREST

When encountering an arrest or prolonged detention situation, officers should make reasonable attempts to determine if the arrestee is responsible for children or dependent adults. In some cases this may be obvious, such as when children or dependent adults are present. However, officers should inquire if the arrestee has caregiver responsibilities for any children or dependent adults who are without appropriate supervision. The following steps should be taken:

- (a) Inquire about and confirm the location of any children or dependent adults.
- (b) Look for evidence of children and dependent adults. Officers should be mindful that some arrestees may conceal the fact that they have a dependent for fear the individual may be taken from them.
- (c) Consider inquiring of witnesses, neighbors, friends and relatives of the arrestee as to whether the person is responsible for a child or dependent adult.

Whenever reasonably possible, officers should take reasonable steps to accomplish the arrest of a parent, guardian or caregiver out of the presence of his/her child or dependent adult. Removing children or dependent adults from the scene in advance of the arrest will generally ensure the best outcome for the individual.

Whenever it is safe to do so, officers should allow the parent or caregiver to assure children or dependent adults that they will be provided care. If this is not safe or if the demeanor of the parent or caregiver suggests this conversation would be non-productive, the officer at the scene should explain the reason for the arrest in age-appropriate language and offer reassurance to the child or dependent adult that he/she will receive appropriate care.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Child and Dependent Adult Safety

338.3.1 AFTER AN ARREST

Whenever an arrest is made, the officer should take all reasonable steps to ensure the safety of the arrestee's disclosed or discovered children or dependent adults.

Officers should allow the arrestee reasonable time to arrange for care of children and dependent adults. Temporary placement with family or friends may be appropriate. However, any decision should give priority to a care solution that is in the best interest of the child or dependent adult. In such cases the following guidelines should be followed:

- (a) Allow the person reasonable time to arrange for the care of children and dependent adults with a responsible party, as appropriate.
 - 1. Officers should consider allowing the person to use his/her cell phone to facilitate arrangements through access to contact phone numbers, and to lessen the likelihood of call screening by the recipients due to calls from unknown sources.
- (b) Unless there is evidence to the contrary (e.g., signs of abuse, drug use, unsafe environment), officers should respect the parent or caregiver's judgment regarding arrangements for care. It is generally best if the child or dependent adult remains with relatives or family friends that he/she knows and trusts because familiarity with surroundings and consideration for comfort, emotional state and safety are important.
 - 1. Except when a court order exists limiting contact, the officer should attempt to locate and place children or dependent adults with the non-arrested parent, guardian or caregiver.
- (c) Provide for the immediate supervision of children or dependent adults until an appropriate caregiver arrives.
- (d) Notify Child Protective Services, if appropriate.
- (e) Notify the field supervisor or Watch Commander of the disposition of children or dependent adults.

If children or dependent adults are at school or another known location outside the household at the time of arrest, the arresting officer should attempt to contact the school or other known location and inform the principal or appropriate responsible adult of the caregiver's arrest and of the arrangements being made for the care of the arrestee's dependent. The result of such actions should be documented in the associated report.

338.3.2 DURING THE BOOKING PROCESS

During the booking process the arrestee shall be allowed to make additional telephone calls to relatives or other responsible individuals as is reasonably necessary to arrange for the care of any child or dependent adult. These telephone calls should be given as soon as practicable and are in addition to any other telephone calls allowed by law.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Child and Dependent Adult Safety

If an arrestee is unable to resolve the care of any child or dependent adult through this process, a supervisor should be contacted to determine the appropriate steps to arrange for care. These steps may include additional telephone calls or contacting a local, county or state services agency.

338.3.3 REPORTING

- (a) For all arrests where children are present or living in the household, the reporting member will document the following information:
 - 1. Name
 - 2. Sex
 - 3. Age
 - 4. Special needs (e.g., medical, mental health)
 - 5. How, where and with whom or which agency the child was placed
 - 6. Identities and contact information for other potential caregivers
 - 7. Notifications made to other adults (e.g., schools, relatives)
- (b) For all arrests where dependent adults are present or living in the household, the reporting member will document the following information:
 - 1. Name
 - 2. Sex
 - 3. Age
 - 4. Whether he/she reasonably appears able to care for him/herself
 - 5. Disposition or placement information if he/she is unable to care for him/herself

338.3.4 SUPPORT AND COUNSELING REFERRAL

If, in the judgment of the handling officers, the child or dependent adult would benefit from additional assistance, such as counseling services, contact with a victim advocate or a crisis telephone number, the appropriate referral information may be provided.

338.4 DEPENDENT WELFARE SERVICES

Whenever an arrestee is unwilling or incapable of arranging for the appropriate care of any child or dependent adult, the handling officer should contact the appropriate welfare service or other department-approved social service to determine whether protective custody is appropriate.

Only when other reasonable options are exhausted should a child or dependent adult be transported to the police facility, transported in a marked law enforcement vehicle or taken into formal protective custody.

Under no circumstances should a child or dependent adult be left unattended or without appropriate care.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Child and Dependent Adult Safety

338.5 TRAINING

The Training Coordinator is responsible to ensure that all members of this department who may be involved in arrests affecting children or dependent adults receive approved training on effective safety measures when a parent, guardian or caregiver is arrested.

Volunteer Program

339.1 PURPOSE AND SCOPE

It is the policy of this department to use qualified volunteers for specified tasks and duties in order to create efficiencies for the Department and improve services to the community. Volunteers are intended to supplement and support, rather than supplant, sworn officers and civilian personnel. Volunteers can be an important part of any organization and have proven to be a valuable asset to law enforcement agencies. Volunteers help to increase departmental responsiveness, delivery of services and information input, and provide new program opportunities. In addition, volunteers bring new skills and expertise to the Department and prompt new enthusiasm.

339.1.1 DEFINITION OF VOLUNTEER

An individual who performs a service for the Department without promise, expectation or receipt of compensation for services rendered. This may include unpaid chaplains, unpaid reserve officers, interns, persons providing administrative support and youth involved in a law enforcement Explorer Post, among others.

339.2 VOLUNTEER MANAGEMENT

339.2.1 VOLUNTEER COORDINATOR

The Volunteer Coordinator shall be appointed by the Deputy Chief of Police. The function of the Volunteer Coordinator is to provide a central coordinating point for effective volunteer management within the Department, and to direct and assist staff and volunteer efforts to jointly provide more productive services. The Volunteer Coordinator should work with other Department staff on an ongoing basis to assist in the development and implementation of volunteer-staffed positions.

The Volunteer Coordinator, or his/her designee, shall be responsible for the following:

- (a) Recruiting, selecting and training qualified volunteers for various positions.
- (b) Facilitating the implementation of new volunteer activities and assignments.
- (c) Maintaining records for each volunteer.
- (d) Tracking and evaluating the contribution of volunteers.
- (e) Maintaining the volunteer handbook and outlining expectations, policies and responsibilities for all volunteers.
- (f) Maintaining a record of volunteer schedules and work hours.
- (g) Completion and dissemination as appropriate of all necessary paperwork and information.
- (h) Planning periodic recognition events.
- (i) Administering discipline when warranted.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Volunteer Program

- (j) Maintaining liaison with other volunteer-utilizing programs in the community and assisting in community-wide efforts to recognize and promote volunteering.

339.2.2 RECRUITMENT

Volunteers should be recruited on a continuous and ongoing basis consistent with department policy on equal opportunity nondiscriminatory employment. A primary qualification for participation in the application process should be an interest in, and an ability to assist the Department in serving the public.

Requests for volunteers should be submitted in writing by interested staff to the Volunteer Coordinator through the requester's immediate supervisor. A complete position description and a requested time frame should be included in the request. All parties should understand that the recruitment of volunteers is enhanced by creative and interesting assignments. The Volunteer Coordinator may withhold assignment of any volunteer until such time as the requesting unit is prepared to make effective use of volunteer resources.

339.2.3 SCREENING

All prospective volunteers should complete the volunteer application form. The Volunteer Coordinator or designee should conduct a face-to-face interview with an applicant under consideration.

A documented background investigation shall be completed on each volunteer applicant and shall include, but not necessarily be limited to, the following:

- (a) Traffic and criminal background check. Fingerprints shall be obtained from all applicants and processed through the Utah Department of Public Safety.
- (b) Employment.
- (c) References.
- (d) Credit check.

A polygraph exam may be required of each applicant depending on the type of assignment.

339.2.4 SELECTION AND PLACEMENT

Service as a volunteer with the Department shall begin with an official notice of acceptance or appointment to a volunteer position. Notice may only be given by an authorized representative of the Department, who will normally be the Volunteer Coordinator. No volunteer should begin any assignment until they have been officially accepted for that position and completed all required screening and paperwork. At the time of final acceptance, each volunteer should complete all required enrollment paperwork and will receive a copy of their position description and agreement of service with the Department. All volunteers shall receive a copy of the volunteer handbook and shall be required to sign a volunteer agreement.

Volunteers should be placed only in assignments or programs that are consistent with their knowledge, skills, abilities and the needs of the Department.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Volunteer Program

339.2.5 TRAINING

Volunteers will be provided with an orientation program to acquaint them with the Department, personnel, policies and procedures that have a direct impact on their work assignment.

Volunteers should receive position-specific training to ensure they have adequate knowledge and skills to complete tasks required by the position and should receive periodic ongoing training as deemed appropriate by their supervisor or the Volunteer Coordinator. Training should reinforce to volunteers that they may not intentionally represent themselves as, or by omission infer that they are sworn officers or other full-time members of the Department. They shall always represent themselves as volunteers.

All volunteers shall comply with the rules of conduct and with all orders and directives, either oral or written, issued by the Department.

339.2.6 FITNESS FOR DUTY

No volunteer shall report to work or be on-duty when his/her judgment or physical condition has been impaired by alcohol, medication, other substances, illness or injury.

Volunteers shall report to their supervisor any changes in status that may affect their ability to fulfill their duties. This includes, but is not limited to, the following:

- (a) Driver's license
- (b) Medical condition
- (c) Arrests
- (d) Criminal investigations

All volunteers shall adhere to the guidelines set forth by this department regarding drug and alcohol use.

339.2.7 DRESS CODE

As representatives of the Department, volunteers are responsible for presenting a professional image to the community. Volunteers shall dress appropriately for the conditions and performance of their duties.

Volunteers shall conform to department-approved dress consistent with their duty assignment. Uniforms authorized for volunteers should be readily distinguishable from those worn by sworn officers. The uniform or identifiable parts of the uniform shall not be worn while off-duty except volunteers may choose to wear the uniform while in transit to or from official department assignments or functions provided an outer garment is worn over the uniform shirt so as not to bring attention to the volunteer while he/she is off duty.

Volunteers shall be required to return any issued uniform or department property at the termination of service.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Volunteer Program

339.3 SUPERVISION OF VOLUNTEERS

Each volunteer who is accepted to a position with the Department must have a clearly identified supervisor who is responsible for direct management of that volunteer. This supervisor will be responsible for day-to-day management and guidance of the work of the volunteer and should be available to the volunteer for consultation and assistance.

A volunteer may be assigned as and act as a supervisor of other volunteers provided that the supervising volunteer is under the direct supervision of a paid staff member.

Functional supervision of volunteers is the responsibility of the supervisor in charge of the unit where the volunteer is assigned. Following are some considerations to keep in mind while supervising volunteers:

- (a) Take the time to introduce volunteers to employees on all levels.
- (b) Ensure volunteers have work space and necessary office supplies.
- (c) Make sure the work is challenging. Do not hesitate to give them an assignment or task that will tap these valuable resources.

339.4 CONFIDENTIALITY

With appropriate security clearance, volunteers may have access to confidential information such as criminal histories or investigative files. Unless otherwise directed by a supervisor or departmental policy, all information shall be considered confidential. Only that information specifically identified and approved by authorized personnel shall be released. Confidential information shall be given only to persons who have a need and a right to know as determined by departmental policy and supervisory personnel.

Each volunteer will be required to sign a nondisclosure agreement before being given an assignment with the Department. Subsequent unauthorized disclosure of any confidential information, verbally, in writing or by any other means, by the volunteer is grounds for immediate dismissal and possible criminal prosecution.

Volunteers shall not address public gatherings, appear on radio or television, prepare any article for publication, act as correspondents to a newspaper or other periodical, release or divulge any information concerning the activities of the Department, or maintain that they represent the Department in such matters without permission from the proper department personnel.

339.5 PROPERTY AND EQUIPMENT

Volunteers will be issued an identification card that must be worn at all times while on-duty. Any fixed and portable equipment issued by the Department shall be for official and authorized use only. Any property or equipment issued to a volunteer shall remain the property of the Department and shall be returned at the termination of service.

339.5.1 VEHICLE USE

Volunteers assigned to duties such as vacation house checks or other assignments that require the use of a vehicle must first complete the following:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Volunteer Program

- (a) A driving safety briefing and department approved driver safety course.
- (b) Verification that the volunteer possesses a valid Utah Driver's License.
- (c) Verification that the volunteer carries current vehicle insurance.

The Volunteer Coordinator should insure that all volunteers receive safety briefing updates and license and insurance verification at least once a year.

When operating a Department vehicle, volunteers shall obey all rules of the road, including seat belt requirements. Smoking is prohibited in all Department vehicles.

Volunteers should not operate a marked patrol car unless there is a prominently placed sign indicating that it is out of service and are not authorized to operate a Department vehicle Code-3.

339.5.2 RADIO AND MDT USAGE

Volunteers shall successfully complete Utah Criminal Justice Information System (UCJIS) and radio procedures training prior to using the police radio or MDT and comply with all related provisions. The Volunteer Coordinator should ensure that radio and UCJIS training is provided for volunteers whenever necessary.

339.6 DISCIPLINARY PROCEDURES/TERMINATION

A volunteer may be removed from the volunteer program at the discretion of the Chief of Police or the Volunteer Coordinator. Volunteers shall have no property interests in their continued appointment. However, if a volunteer is removed for alleged misconduct, the volunteer will be afforded an opportunity solely to clear his/her name through a liberty interest hearing which shall be limited to a single appearance before the Chief of Police or authorized designee.

Volunteers may resign from volunteer service with the Department at any time. It is requested that volunteers who intend to resign provide advance notice of their departure and a reason for their decision.

339.6.1 EXIT INTERVIEWS

Exit interviews, where possible, should be conducted with volunteers who are leaving their positions. The interview should ascertain why the volunteer is leaving the position and solicit the volunteer's suggestions on improving the position. When appropriate, the interview should also include a discussion on the possibility of involvement in some other capacity with the Department.

339.7 EVALUATION

An evaluation of the overall volunteer program will be conducted on an annual basis by the Volunteer Coordinator. Regular evaluations should be conducted with volunteers to ensure the best use of human resources available, to ensure personnel problems can be identified and dealt with promptly and fairly, and to ensure optimum satisfaction on the part of volunteers.

Off-Duty Law Enforcement Actions

340.1 PURPOSE AND SCOPE

The decision to become involved in a law enforcement action when off-duty can place an officer as well as others at great risk and must be done with careful consideration. This policy is intended to provide guidelines for officers of the South Salt Lake Police Department with respect to taking law enforcement action while off-duty.

340.2 POLICY

Initiating law enforcement action while off-duty is generally discouraged. Officers should not attempt to initiate enforcement action when witnessing minor crimes, such as suspected intoxicated drivers, reckless driving or minor property crimes. Such incidents should be promptly reported to the appropriate law enforcement agency.

Officers are not expected to place themselves in unreasonable peril. However, any sworn member of this department who becomes aware of an incident or circumstance that he/she reasonably believes poses an imminent threat of serious bodily injury or death, or significant property damage may take reasonable action to minimize the threat.

When public safety or the prevention of major property damage requires immediate action, officers should first consider reporting and monitoring the activity and only take direct action as a last resort.

Officers should remember that their authority as a peace officer may not extend to actions taken outside their jurisdiction unless authorized by law (Utah Code § 77-9-3).

340.3 FIREARMS

Officers of this department may carry firearms while off-duty in accordance with federal regulations and department policy. All firearms and ammunition must meet guidelines as described in the department Firearms Policy. When carrying firearms while off-duty, officers shall also carry their department-issued badge and identification.

Officers should refrain from carrying firearms when the consumption of alcohol is likely or when the need to carry a firearm is outweighed by safety considerations. Firearms shall not be carried by any officer who has consumed an amount of an alcoholic beverage, taken any drugs or medications or any combination thereof that would tend to adversely affect the officer's senses or judgment.

340.4 DECISION TO INTERVENE

There is no legal requirement for off-duty officers to take law enforcement action. However, should officers decide to intervene, they must evaluate whether the action is necessary or desirable, and should take into consideration the following:

- (a) The tactical disadvantage of being alone and the fact there may be multiple or hidden suspects.
- (b) The inability to communicate with responding units.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Off-Duty Law Enforcement Actions

- (c) The lack of equipment, such as handcuffs, OC or baton.
- (d) The lack of cover.
- (e) The potential for increased risk to bystanders if the off-duty officer were to intervene.
- (f) Unfamiliarity with the surroundings.
- (g) The potential for the off-duty officer to be misidentified by other peace officers or members of the public.

Officers should consider waiting for on-duty uniformed officers to arrive, and gather as much accurate intelligence as possible instead of immediately intervening.

340.4.1 INTERVENTION PROCEDURE

If involvement is reasonably necessary, the officer should attempt to call or have someone else call 9-1-1 to request immediate assistance. The operator should be informed that an off-duty officer is on-scene and should be provided a description of the officer if possible.

Whenever practicable, the officer should loudly and repeatedly identify him/herself as an South Salt Lake Police Department officer until acknowledged. Official identification should also be displayed.

340.4.2 INCIDENTS OF PERSONAL INTEREST

Officers should refrain from handling incidents of personal interest, (e.g., family or neighbor disputes) and should remain neutral. In such circumstances officers should call the responsible agency to handle the matter.

340.4.3 NON-SWORN RESPONSIBILITIES

Non-sworn personnel should not become involved in any law enforcement actions while off-duty except to notify the local law enforcement authority and remain at the scene, if safe and practicable.

340.4.4 OTHER CONSIDERATIONS

When encountering a non-uniformed officer in public, uniformed officers should wait for acknowledgement by the non-uniformed officer in case he/she needs to maintain an undercover capability.

340.5 REPORTING

Any officer, prior to taking any off-duty enforcement action, shall notify and receive approval of an South Salt Lake Police Department Supervisor (or other applicable law enforcement authority if acting outside the jurisdiction of the South Salt Lake Police Department). If prior contact is not reasonably possible, an officer shall notify the applicable local law enforcement agency as soon as reasonably possible (Utah Code § 77-9-3). The Watch Commander shall determine whether a report should be filed by the employee.

Officers should cooperate fully with the agency having jurisdiction in providing statements or reports as requested or as appropriate.

Community Relations

341.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for community relationship-building.

Additional guidance on community relations and outreach is provided in other policies, including the:

- Hate Crimes Policy.
- Limited English Proficiency Services Policy.
- Communications with Persons with Disabilities Policy
- Patrol Function Policy.
- Suspicious Activity Reporting Policy.

341.2 POLICY

It is the policy of the South Salt Lake Police Department to promote positive relationships between department members and the community by treating community members with dignity and respect and engaging them in public safety strategy development and relationship-building activities, and by making relevant policy and operations information available to the community in a transparent manner.

341.3 MEMBER RESPONSIBILITIES

Officers should, as time and circumstances reasonably permit:

- (a) Make casual and consensual contacts with community members to promote positive community relationships (see the Detentions and Photographing Detainees Policy).
- (b) Become reasonably familiar with the schools, businesses and community groups in their assigned jurisdictional areas.
- (c) Work with community members and the department community resource unit to identify issues and solve problems related to community relations and public safety.
- (d) Conduct periodic foot patrols of their assigned areas to facilitate interaction with community members. Officers carrying out foot patrols should notify an appropriate supervisor and Dispatch of their status (i.e., on foot patrol) and location before beginning and upon completion of the foot patrol. They should also periodically inform Dispatch of their location and status during the foot patrol.

341.4 COMMUNITY OUTREACH COORDINATOR

The Chief of Police or the authorized designee should designate a member of the Department to serve as the community outreach coordinator. The Community Outreach Coordinator should report directly to the Chief of Police or the authorized designee and is responsible for:

- (a) Obtaining department-approved training related to responsibilities.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Community Relations

- (b) Responding to requests from department members and the community for assistance in identifying issues and solving problems related to community relations and public safety.
- (c) Work with the administrative lieutenant to coordinate community engagements, surveys, and events.
- (d) The Community Outreach Coordinator is the primary liaison with the civil review board.
- (e) Working with community groups, department members and other community resources to:
 - (a) Identify and solve public safety problems within the community.
 - (b) Organize programs and activities that help build positive relationships between department members and the community and provide community members with an improved understanding of department operations
- (f) Create content to recognizing department and community members for exceptional work or performance in community relations efforts.
- (g) Attending City council and other community meetings to obtain information on community relations needs as assigned by the deputy chief or chief of police.
- (h) Assisting with the department's response to events that may affect community relations, such as an incident where the conduct of a department member is called into public question.
- (i) Informing the Chief of Police and others of developments and needs related to the furtherance of the department's community relations goals, as appropriate.

341.5 SURVEYS

The community relations coordinator should arrange for a survey of community members and department members to be conducted at least annually to assess the condition of the relationship between the Department and the community. Survey questions should be designed to evaluate perceptions of the following:

- (a) Overall performance of the Department
- (b) Overall competence of department members
- (c) Attitude and behavior of department members
- (d) Level of community trust in the Department
- (e) Safety, security or other concerns

A written summary of the compiled results of the survey should be provided to the Chief of Police.

341.6 COMMUNITY AND YOUTH ACTIVITIES AND PROGRAMS

The community outreach coordinator should assist with the School Resource Sergeant to assist with programs and activities that create opportunities for department members and community members, especially youths, to interact in a positive setting. Examples of such programs and events include:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Community Relations

- (a) Department-sponsored athletic programs (e.g., baseball, basketball, soccer, bowling).
- (b) Police-community get-togethers (e.g., cookouts, meals, charity events).
- (c) Youth leadership and life skills mentoring.
- (d) School resource officer/NOVA Instructor.
- (e) Neighborhood watches and crime prevention programs.

341.7 INFORMATION SHARING

The community outreach coordinator should work with the Public Information Officer to develop methods and procedures for the convenient sharing of information (e.g., major incident notifications, significant changes in department operations, comments, feedback, positive events) between the Department and community members. Examples of information-sharing methods include:

- (a) Community meetings.
- (b) Social media (see the Department Use of Social Media Policy).
- (c) Department website postings.

Information should be regularly refreshed, to inform and engage community members continuously.

341.8 LAW ENFORCEMENT OPERATIONS EDUCATION

The community outreach coordinator should help develop methods or create content to educate community members on general law enforcement operations so they may understand the work that officers do to keep the community safe. Examples of educational methods include:

- (a) Development and distribution of informational cards/flyers.
- (b) Department website postings.
- (c) Presentations to driver education classes.
- (d) Instruction in schools.
- (e) Department ride-alongs (see the Ride-Along Program Policy).
- (f) Scenario/Simulation exercises with community member participation.
- (g) Youth internships at the department.
- (h) Citizen academies.

Instructional information should include direction on how community members should interact with the police during enforcement or investigative contacts and how community members can make a complaint to the department regarding alleged misconduct or inappropriate job performance by department members.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Community Relations

341.9 SAFETY AND OTHER CONSIDERATIONS

Department members responsible for community relations activities should consider the safety of the community participants and, as much as reasonably practicable, not allow them to be present in any location or situation that would jeopardize their safety.

Department members in charge of community relations events should ensure that participating community members have completed waiver forms before participation, if appropriate. A parent or guardian must complete the waiver form if the participating community member has not reached 18 years of age.

Community members are subject to a criminal history check before approval for participation in certain activities, such as citizen academies, or engaging youth.

341.10 COMMUNITY ADVISORY COMMITTEE

The Chief of Police should establish a committee of volunteers consisting of community members, community leaders and other community stakeholders (e.g., representatives from schools, churches, businesses, social service organizations). The makeup of the committee should reflect the demographics of the community as much as practicable.

The committee should convene regularly to:

- (a) Provide a public forum for gathering information about public safety concerns in the community.
- (b) Work with the Department to develop strategies to solve public safety problems.
- (c) Generate plans for improving the relationship between the department and the community.
- (d) Participate in community outreach to solicit input from community members, including youths from the community.

The Training Coordinator should arrange for initial and ongoing training for committee members on topics relevant to their responsibilities.

The Chief of Police may include the committee in the evaluation and development of department policies and procedures and may ask them to review certain personnel complaints for the purpose of providing recommendations regarding supervisory, training or other issues as appropriate.

341.10.1 LEGAL CONSIDERATIONS

The Chief of Police and the community relations coordinator should work with the City Attorney as appropriate to ensure the committee complies with any legal requirements such as public notices, records maintenance and any other associated obligations or procedures.

341.11 TRANSPARENCY

The Department should periodically publish statistical data and analysis regarding the department's operations. The reports should not contain the names of officers, suspects or case numbers. The community relations coordinator should work with the community

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Community Relations

advisory committee to identify information that may increase transparency regarding department operations.

341.12 TRAINING

Subject to available resources, members should receive training related to this policy, including training on topics such as:

- (a) Effective social interaction and communication skills.
- (b) Cultural, racial and ethnic diversity and relations.
- (c) Building community partnerships.
- (d) Community policing and problem-solving principles.
- (e) Enforcement actions and their effects on community relations.

Where practicable and appropriate, community members, especially those with relevant expertise, should be involved in the training to provide input from a community perspective.

Generative Artificial Intelligence Use

342.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for [department/office] use of generative artificial intelligence (GenAI). This policy does not apply to artificial intelligence that is integrated into facial recognition applications, voice recognition applications, biometric access controls, or software that redacts documents or video or similar applications (Utah Code 53-25-902).

Additional guidelines for the use of [department/office] information technology resources are found in the Information Technology Use Policy.

342.1.1 DEFINITIONS

Definitions related to this policy include:

Artificial intelligence- means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.

Generative artificial intelligence (GenAI) - means artificial intelligence that is capable of creating content such as text, audio, image, or video based on patterns learned from large volumes of data rather than being explicitly programed with rules. A type of artificial intelligence that is algorithmically trained on one or more large data sets and designed to generate new and unique data (e.g., text, pictures, video) in response to a prompt (generally questions, instructions, images, or video) input by the user (Utah Code 53-25-901).

342.2 POLICY

The use of GenAI systems carries unique benefits within a law enforcement agency, providing ways to increase operational efficiency, enhance [department/office] procedures, and improve the overall effectiveness of the South Salt Lake Police Department

However, the prompts input into GenAI systems can present risks to both individuals and law enforcement agencies by making information accessible to the public such as [department/office] tactics, investigative and training techniques, confidential information (e.g., confidential informants, protected information), active investigations, and security procedures. In addition, without safeguards in place, GenAI can produce unintended discriminatory or biased output as well as content that is inaccurate, misleading, or copyrighted.

It is the policy of the [Department/Office] to develop, implement, and use GenAI ethically and responsibly in a way that minimizes potential risk and harm in accordance with the guidelines set forth below.

Any function carried out by a member of the Department using GenAI is subject to the same laws, rules, and policies as if carried out without the use of GenAI. The use of GenAI does not permit any law, rule, or policy to be bypassed or ignored.

342.3 RESPONSIBILITIES

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Generative Artificial Intelligence Use

342.3.1 CHIEF OF POLICE

The Chief of Police or an authorized designee shall approve all GenAI systems, their acceptable uses, and their authorized user groups prior to the use, implementation, or development for any department functions.

342.3.2 AI COORDINATOR

The Chief of Police or the authorized designee shall appoint an AI coordinator. The AI coordinator shall report to the Chief of Police or the authorized designee.

The responsibilities of the AI coordinator include but are not limited to:

- (a) Evaluating potential GenAI systems and recommending those GenAI systems that appear to be appropriate and trustworthy to the Chief of Police or the authorized designee. The trustworthiness of GenAI systems should be evaluated by balancing the following characteristics:
 - 1. Validity and reliability - The system's apparent ability to meet the intended purpose and fulfill the needs of the department consistently over time.
 - 2. Safety - Any apparent risk to human life, health, property, or the environment that could result from the [department/office]'s use of the system.
 - 3. Security and resiliency - The system's capability to prevent unauthorized access and misuse and its ability to return to normal function should misuse occur.
 - 4. Accountability and transparency - The ability to track and measure the system's use and activity through histories, audit logs, and other processes to provide insight about the system and identify potential sources of error, bias, or vulnerability.
 - 5. Explainability and interpretability - The ability of the user to understand the purpose and impact of the system, how and why the system reached the resulting output, and what the output means for the user.
 - 6. Privacy - The ability of the system to protect confidentiality and meet applicable privacy standards for the types of data intended to be input into the system (e.g., state privacy laws such as the Utah Governmental Data Privacy Act (GDPA), Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA)).
 - 7. Fairness - The ability of the system to operate in a way that avoids or minimizes bias and discrimination.
- (b) Ensuring appropriate contractual safeguards are in place to manage third-party use of department data and to restrict the use of input in AI training data sets. If the input of protected information is necessary for the proper use of the GenAI system, the appropriate user agreement, management control agreement, an information-exchange agreement, and CJIS security addendums must be maintained and utilized in compliance with applicable rules and standards (e.g., CJIS requirements) and should be used to outline the roles, responsibilities, and data ownership between the department and third-party vendor.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Generative Artificial Intelligence Use

- (c) Coordinating with others within the department and South Salt Lake City, such as the information technology or legal departments, as appropriate to ensure GenAI systems are procured, implemented, and used appropriately.
- (d) Maintaining a list or inventory of department-approved GenAI systems.[department/office]
- (e) Developing and maintaining appropriate procedures related to the use of GenAI systems, including procedures for editing and fact-checking output.
- (f) Ensuring any public-facing GenAI systems notify the user that GenAI is being used.
- (g) Developing and updating training for the authorized users of each department-approved GenAI system.
- (h) Ensuring access to [department/office] GenAI systems is limited to authorized users and establishing requirements for user credentials such as two-factor authentication and appropriate password parameters.
- (i) Conducting audits at reasonable time intervals for each of the GenAI systems utilized by the [Department/Office] to evaluate the performance and effectiveness of each approved system and to determine if it continues to meet the [department/office]'s needs and expectations of trustworthiness. The coordinator should arrange for audits to be conducted by an external source, as needed.
- (j) Ensuring each GenAI system is updated and undergoes additional training as reasonably appears necessary in an effort to avoid the use of outdated information or technologies.
- (k) Keeping abreast of advancements in GenAI and any GenAI-related legal developments.
- (l) Reviewing this policy and [department/office] practices and proposing updates as needed to the Chief of Police.
- (m) Developing procedures in coordination with the *Brady* information coordinator and the Records Supervisor for the compilation and potential release of any discovery or records related to the use of GenAI systems consistent with *Brady* and the Utah Government Records Access and Management Act.

342.4 USE OF GENERATIVE AI

The use of [department/office] GenAI systems by [department/office] members shall be limited to official work-related purposes, and members shall only access and use GenAI systems for which they have been authorized and received proper training (Utah Code 53-25-902).

Members shall use AI-generated content as an informational tool and not as a substitution for human judgment or decision-making. Members should not represent AI-generated content as their own original work.

AI-generated content should be considered draft material only and shall be thoroughly reviewed prior to use. Before relying on AI-generated content, members should:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Generative Artificial Intelligence Use

- (a) Obtain independent sources for information provided by GenAI and take reasonable steps to verify that the facts and sources provided by GenAI are correct and reliable.
- (b) Review prompts and output for indications of bias and discrimination and take steps to mitigate its inclusion when reasonably practicable (see the Bias-Based Policing Policy).

342.4.1 PRIVACY CONSIDERATIONS

Information not otherwise available to the public, including data reasonably likely to compromise an investigation, reveal confidential law enforcement techniques, training, or procedures, or risk the safety of any individual if it were to become publicly accessible, should not be input into a GenAI system unless contractual safeguards are in place to prevent such information from becoming publicly accessible. Members should instead use generic unidentifiable inputs, such as "suspect" or "victim," and hypothetical scenarios whenever possible.

Protected information should only be input into GenAI systems that have been approved for such use and comply with applicable privacy laws and standards (see the Protected Information Policy).

342.4.2 DISCLAIMER AND CERTIFICATION

Any final document or work product created by a member using GenAI shall include a disclaimer that it contains content generated by artificial intelligence and a certification that it has been read and reviewed by the author for accuracy (Utah Code 53-25-902).

342.5 PROHIBITED USE

Members shall not use GenAI systems to rationalize a law enforcement decision, or as the sole basis of research, interpretation, or analysis of the law or facts related to a law enforcement contact or investigation.

Members shall not create user accounts in their official capacity or input work-related data (including information learned solely in the scope of their employment) into publicly available GenAI systems unless the system has been approved by the Chief of Police or the authorized designee for the intended use.

Any member who fails to comply with the requirement of the policy may be subject to discipline, up to including termination.

342.6 TRAINING

The AI coordinator should ensure that all members authorized to use GenAI have received appropriate initial training that is suitable for their role and responsibilities prior to their use of GenAI and receive periodic refresher training. Training should include but is not limited to the following:

- (a) A review of this policy
- (b) The need for human oversight of GenAI outputs
- (c) The interpretation, review, and verification of GenAI output
- (d) Checking GenAI output for bias or protected information

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Generative Artificial Intelligence Use

- (e) Ethical use of GenAI technology
- (f) Data security and privacy concerns

ADA Compliance

343.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for equal access to South Salt Lake Police Department services, programs, and activities for persons with disabilities, in accordance with Title II of the Americans with Disabilities Act (ADA).

This policy also includes guidelines to provide effective communication with persons with disabilities. See the Service Animals Policy for guidance on protecting the rights of individuals who use service animals in accordance with the ADA.

343.1.1 DEFINITIONS

Definitions related to this policy include (28 CFR 35.104):

ADA coordinator - The member designated by the Chief of Police to coordinate the department's efforts to comply with the ADA (28 CFR 35.107).

Assistive devices, auxiliary aids, and services - Tools used by persons with disabilities to facilitate their participation in services, programs, and activities offered by the South Salt Lake Police Department and to facilitate effective communication. They include but are not limited to the use of gestures or visual aids to supplement oral communication; a notepad and pen or pencil to exchange written notes; a computer or typewriter; an assistive listening system or device to amplify sound; a teletypewriter (TTY) or videophones (video relay service or VRS); taped text; a qualified reader; or a qualified interpreter.

Disability - A physical or mental impairment that substantially limits a major life activity including hearing, seeing, or speaking, regardless of whether the person uses assistive devices, auxiliary aids, and services. Individuals who wear ordinary eyeglasses or contact lenses are not considered to have a disability (42 USC § 12102; 28 CFR 35.108).

Facility - All aspects of [department/office] buildings, structures, sites, complexes, equipment, rolling stock or other conveyances, roads, walkways, parking areas, and other real or personal property (28 CFR 35.108).

Modification - Any change, adjustment, alteration, adaptation, or accommodation that renders a [department/office] service, program, or activity suitable for use, enjoyment, or participation by a person with a disability. This may include alteration of existing buildings and facilities.

A modification includes any change or exception to a policy, practice, or procedure that allows a person with a disability to have equal access to services, programs, and activities. It also includes the provision or use of assistive devices, auxiliary aids, and services.

Qualified interpreter - A person who is able to interpret effectively, accurately, and impartially, both receptively and expressively, using any necessary specialized vocabulary. Qualified interpreters include oral interpreters, transliterators, sign language interpreters, and intermediary interpreters. Qualified interpreters should have a certification approved by the Utah Division of

South Salt Lake Police Department

South Salt Lake PD Policy Manual

ADA Compliance

Services for the Deaf and Hard of Hearing Interpreters Certification Board (Utah Code 35A-13-605; UAC R993-300-301 et seq.).

343.2 POLICY

It is the policy of the South Salt Lake Police Department that persons with disabilities, including victims, witnesses, suspects, and arrestees, have equal access to services, programs, and activities of the [Department/Office].

The [Department/Office] will not discriminate against or deny any individual access to services, programs, or activities based upon the presence or suspected presence of disabilities.

343.3 ADA COORDINATOR RESPONSIBILITIES

The responsibilities of the ADA coordinator include but are not limited to (28 CFR 35.130):

- (a) Collaborating with the City ADA coordinator regarding the South Salt Lake Police Department's efforts to provide equal access to services, programs, and activities.
 - 1. Maintaining [department/office] compliance with accessibility standards for [department/office] web content and mobile applications as required by 28 CFR 35 Subpart H (28 CFR 35.200).
- (b) Collaborating with the City ADA coordinator to facilitate a process of periodic self-evaluation. The process should include:
 - 1. Inspection of current [department/office] facilities to identify access issues.
 - 2. Review of current [department/office] services, activities, and programs for access issues.
 - 3. Assessment and update, if necessary, of current compliance measures.
 - 4. Identification of recurring areas of complaint for which new methods of modification should be considered.
 - 5. Review of the [department/office]'s emergency programs, services, and activities as they apply to persons with disabilities.
 - 6. Recommendation of a schedule to implement needed improvements.
- (c) Acting as a liaison with local disability advocacy groups or other disability-focused groups regarding access to [department/office] services, programs, and activities.
- (d) Developing procedures that will enable members to access assistive devices, auxiliary aids, and services, and making the procedures available as appropriate.
 - 1. A list of qualified interpreter services with contact and availability information should be maintained and easily accessible to members.
- (e) Developing procedures for the review and processing of requests for modifications that will help members provide persons with disabilities access to [department/office] services, programs, and activities, as appropriate.
- (f) Establishing procedures for the booking process to assist members with managing commonly encountered disabilities such as sight or mobility impairments and intellectual or developmental disabilities.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

ADA Compliance

- (g) Providing notice to the public regarding the rights and protections afforded by the ADA. This may include posters, published notices, handbooks, manuals, and pamphlets describing [department/office] services, programs, and activities and the availability of assistive devices, auxiliary aids, and services, as well as modifications (28 CFR 35.106).
- (h) Collaborating with other [city/county] departments during the planning process to provide that new construction and any alteration to an existing building or facility are undertaken in compliance with the ADA (28 CFR 35.151).
- (i) Developing, implementing, and publishing appropriate procedures to provide for the prompt and equitable resolution of complaints and inquiries regarding discrimination in access to services, programs, and activities. The complaint procedures should include an appeal process (28 CFR 35.107).
- (j) Verifying that third parties providing [department/office] services, programs, or activities through contract, outsourcing, licensing, or other arrangement have established reasonable policies and procedures to prevent discrimination against and denial of access to persons with disabilities.
- (k) Recommending amendments to this policy as needed.

343.4 REQUESTS

The goal of any modification should be to allow a person with a disability to participate in a service, program, or activity the same as a person who does not have a disability.

Upon receiving a request for a modification, members should make reasonable efforts to accommodate the request based on the preference of the person with the disability. Members should not ask about the nature and extent of a person's disability but should limit questions to elicit information necessary to determine the need for a modification and the appropriate type of modification.

If the requested modification or an alternative modification can reasonably be made at the time of the request, the member should make the modification. A member who is unable to accommodate a request or unsure about whether a request should be accommodated should contact a supervisor.

The supervisor should review and approve the request, if practicable and appropriate. Otherwise, the supervisor should document the requesting person's contact information and the modification being requested and forward the request to the ADA coordinator for processing as soon as reasonably practicable.

343.4.1 DENIAL OF A REQUEST

The following should be considered before denying a request for modification:

- (a) Requests for modifications should be approved unless complying with the request would result in (28 CFR 35.150):
 - 1. A substantial alteration of the service, program, or activity.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

ADA Compliance

2. An undue financial or administrative burden on the [Department/Office]. All resources available for use in the funding and operation of the service, program, or activity at issue should be considered in this determination.
 3. A threat to or the destruction of the historic significance of a historic property.
 4. A direct threat to the health or safety of others (28 CFR 35.139).
- (b) If any of these circumstances are present, the ADA coordinator should work with [department/office] members and the person requesting the modification to determine if an alternative modification is available.
- (c) Where new construction or physical modification of an existing building or facility would be unfeasible or unduly burdensome, the ADA coordinator should work with [department/office] members to determine whether alternative modifications are available. Alternative methods that should be considered include (28 CFR 35.150):
1. Reassigning services, programs, or activities to accessible buildings or facilities.
 2. Utilizing technology, equipment, rolling stock, or other conveyances.
 3. Delivering the services, programs, or activities directly to a person with a disability by way of home visits or meeting the person at an accessible location.
 4. Any other means or methods that would make services, programs, or activities readily accessible.
- (d) If no alternative modification is appropriate, the ADA coordinator shall issue a written statement explaining why a modification of the service, program, or activity will not be made (28 CFR 35.150).

343.4.2 PERSONAL DEVICES AND ASSISTANCE

Although members should make every effort to comply with requests, the provision of personal devices or assistance (e.g., wheelchairs, eyeglasses, hearing aids, personal assistance in eating or using the restroom) to persons with disabilities is not required (28 CFR 35.135).

343.4.3 SURCHARGES

Surcharges shall not be imposed upon persons with disabilities to cover the costs of providing modifications (28 CFR 35.130(f)).

343.5 COMMUNICATIONS WITH PERSONS WITH DISABILITIES

Members should remain alert to the possibility of communication problems when engaging with persons with disabilities. When a member knows or suspects an individual requires assistance to effectively communicate, the member should identify the individual's choice of assistive devices, auxiliary aids, and services. The individual's preferred communication method should be honored unless another effective method of communication exists under the circumstances (28 CFR 35.160).

Factors to consider when determining whether an alternative method may be effective include:

- (a) The methods of communication usually used by the individual.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

ADA Compliance

- (b) The nature, length, and complexity of the communication involved.
- (c) The context of the communication.

In emergency situations involving an imminent threat to the safety or welfare of any person, members may use whatever modification reasonably appears effective under the circumstances. This may include exchanging written notes or using the services of a person who knows sign language but is not a qualified interpreter, even if the person who is deaf or hard of hearing would prefer a qualified sign language interpreter. Once the emergency has ended, the method of communication should be reconsidered. The member should inquire as to the individual's preference and give primary consideration to that preference.

343.5.1 TYPES OF ASSISTANCE AVAILABLE

[Department/Office] members shall not refuse an available type of assistive device, auxiliary aid, or service to a person with a disability who is requesting assistance. The [Department/Office] will not require persons with disabilities to furnish their own assistive device, auxiliary aid, or service as a condition for receiving access to [department/office] services, programs, and activities. The [Department/Office] will make every reasonable effort to provide equal access and timely assistance to persons with disabilities through a variety of assistive devices, auxiliary aids, and services (28 CFR 35.160).

The [Department/Office] will not require that persons with disabilities use [department/office]-provided assistive devices, auxiliary aids, and services. [Department/Office]-provided assistive devices, auxiliary aids, and services may include but are not limited to the means described in this policy.

343.5.2 AUDIO RECORDINGS AND ENLARGED PRINT

The [Department/Office] may develop audio recordings to assist people who are blind or have a visual impairment. If such a recording is not available, members may read aloud from the appropriate form or provide forms with enlarged print.

343.5.3 QUALIFIED INTERPRETERS

A qualified interpreter may be needed in lengthy or complex transactions (e.g., interviewing a victim, witness, suspect, or arrestee) with individuals who normally rely on sign language or speechreading (i.e., lip-reading) to understand what others are saying. The qualified interpreter should not be a person with an interest in the matter. A person providing interpretation services may be required to establish the accuracy and trustworthiness of the interpretation in a legal proceeding.

Qualified interpreters should be:

- (a) Available within a reasonable amount of time.
- (b) Experienced in providing interpretation services related to law enforcement matters in the person's primary language.
- (c) Familiar with the use of text- and video-based communications products and systems.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

ADA Compliance

- (d) Certified in either American Sign Language (ASL) or Signing Exact English (SEE).
- (e) Able to understand and adhere to the interpreter role without deviating into other roles, such as counselor or legal adviser.
- (f) Knowledgeable of the ethical issues involved when providing interpreter services.

Members should use [department/office]-approved procedures to request a qualified interpreter at the earliest reasonable opportunity or when it is reasonably apparent that an interpreter is needed. The use of a video remote interpreting service should be considered, where appropriate, if a live interpreter is not available. Persons with disabilities shall not be required to provide an interpreter (28 CFR 35.160).

343.5.4 TELECOMMUNICATION SERVICES

In situations where an individual without a disability would have access to a telephone (e.g., during booking or attorney contacts), members must also provide those with communication-related disabilities the opportunity to place calls using an available TTY, TDD, or other voice, text, or video-based communications product or system. Members shall provide additional time, as needed, for effective communication due to the slower nature of assisted communications.

The [Department/Office] will accept all TDD and computer modem calls placed by individuals with communications-related disabilities and received via a telecommunications relay service (28 CFR 35.162).

343.5.5 COMMUNITY VOLUNTEERS

Where qualified interpreters are unavailable to assist members, [department/office]-approved community volunteers who have demonstrated competence in communication services, such as ASL or SEE, may be called upon to provide interpreter services when appropriate. However, [department/office] members must carefully consider the nature of the interaction and the relationship between the individual with the disability and the volunteer to be reasonably satisfied that the volunteer can provide neutral and unbiased assistance.

343.5.6 FAMILY AND FRIENDS

While family or friends may offer to assist with interpretation, members should carefully consider the circumstances before relying on such individuals. The nature of the interaction and relationship between the individual with the disability and the person offering services must be carefully considered to determine whether the family member or friend can provide neutral and unbiased assistance.

Except in an emergency involving an imminent threat to the safety or welfare of any person and no qualified interpreter is reasonably available, members shall not use a minor child as an interpreter (28 CFR 35.160).

343.5.7 FIELD ENFORCEMENT CONSIDERATIONS

Due to the unpredictable and varied nature of field enforcement, the [Department/Office] recognizes that it is impracticable to provide immediate access to a comprehensive supply

South Salt Lake Police Department

South Salt Lake PD Policy Manual

ADA Compliance

of assistive devices, auxiliary aids, and services to every member of this [department/office]. Members involved in interactions with persons with disabilities that occur in the field should assess each situation to determine if communication assistance is necessary. The length, complexity, and importance of the communication, as well as the individual's preferred method of communication, should be considered when determining what, if any, resources should be used and whether a qualified interpreter or other service is needed.

343.6 CUSTODIAL INTERROGATIONS

In an effort to ensure that the rights of individuals with disabilities are protected during a custodial interrogation, this [department/office] will provide reasonable modifications before beginning an interrogation, unless exigent circumstances exist or the individual has made a clear indication that the individual understands the process and desires to proceed without receiving a modification. *Miranda* warnings should be provided to a suspect via the individual's preferred method of communication.

Interrogations should be recorded whenever reasonably practicable. See guidance on recording custodial interrogations in the Investigation and Prosecution Policy.

343.7 ARREST

If an individual with a communication-related disability is arrested, the arresting officer shall use [department/office]-approved procedures to provide a qualified interpreter as soon as reasonably practicable, unless the individual indicates a preference for a different assistive device, auxiliary aid, or service, or the officer reasonably determines another effective method of communication exists under the circumstances.

Individuals who are arrested and are assisted by service animals should be permitted to make arrangements for the care of such animals prior to transport.

343.8 WEBSITE ACCESS

The ADA coordinator should work with the appropriate parties to develop online content that is readily accessible to persons with disabilities. [Department/Office] web content should be developed in conformance with the most current guidelines issued by the U.S. Department of Justice and federal regulations (28 CFR 35 Subpart H; 28 CFR 35.200).

[Department/Office] website content should also be made available to persons with disabilities in an alternative format upon request, if reasonably practicable.

343.9 DOCUMENTATION

Whenever any modification has been provided, the member involved should document:

- (a) The type of modification, assistive device, auxiliary aid, or service provided.
- (b) Whether the individual elected to use an assistive device, auxiliary aid, or service provided by the [Department/Office] or another identified source, as applicable.
- (c) Whether the individual's express preference for the modification was not honored and the reason why an alternative method was used.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

ADA Compliance

The documentation and any written communications exchanged should be maintained consistent with the Records Maintenance and Release Policy.

All written communications exchanged in a criminal case shall be attached to the member's report or placed into evidence.

343.10 COMPLAINTS

A member who receives a complaint or becomes aware of potential disability discrimination, an ADA violation, or a person's inability to access the [department/office]'s programs, services, or activities should document the complaint and promptly refer the matter to the ADA coordinator (28 CFR 35.107). The [Department/Office] shall assist persons with disabilities who require assistance to file a complaint regarding members of this [department/office]. The [Department/Office] may provide a qualified interpreter or forms in enlarged print, as appropriate.

343.11 TRAINING

Members should receive periodic training on ADA compliance, to include:

- (a) Awareness and understanding of this policy, related procedures, forms, and available resources.
- (b) Procedures for handling requests for modifications.
- (c) Accessing assistive devices, auxiliary aids, and services needed to accommodate requests for modifications.
- (d) General requirements of the ADA, including modifying policies and practices, communicating with individuals with disabilities, and identifying alternate ways to provide access to programs, services, and activities as appropriate to the member's job duties.

Management staff, even if they do not interact regularly with individuals with disabilities, should receive training as appropriate to understand and reinforce this policy.

The Training Coordinator should maintain records of all training provided and retain a copy in each member's training file in accordance with the established records retention schedule.

343.11.1 CALL-TAKER TRAINING

Emergency call-takers shall be trained in the use of [department/office] assistive devices, auxiliary aids, and services for communicating with individuals with communication-related disabilities. Such training and information should include:

- (a) The requirements of the ADA and Section 504 of the Rehabilitation Act for telephone emergency service providers.
- (b) ASL syntax and accepted abbreviations.
- (c) Practical instruction on identifying and processing calls using TTY, TDD, or other voice, text, and video-based communications products and systems.
- (d) Hands-on experience in using TTY, TDD, or other voice, text, and video-based communications products and systems.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

ADA Compliance

Training should be provided for all Dispatch members who may have contact with individuals from the public who have communication-related disabilities. Refresher training should be provided as appropriate.

Vehicle Pursuits

344.1 PURPOSE AND SCOPE

This policy provides guidelines for vehicle pursuits in order to protect the safety of involved officers, the public, and fleeing suspects (Utah Code 41-6a-212).

344.1.1 DEFINITIONS

Definitions related to this policy include:

Boxing-in - A low-speed tactic designed to stop a fleeing vehicle by surrounding it with emergency vehicles and then slowing all vehicles to a stop.

Pursuit Intervention Technique (PIT) - A low-speed tactic designed to apply lateral pressure to the rear quarter panel of a fleeing vehicle, causing it to spin out, stall, and come to a stop (also known as a Precision Immobilization Technique).

Ramming - The deliberate act of impacting a fleeing vehicle with another vehicle to functionally damage or otherwise force the fleeing vehicle to stop.

Roadblock - A tactic designed to stop a fleeing vehicle by intentionally placing an emergency vehicle or other immovable object in the path of the fleeing vehicle.

Tire deflation device - A device designed to be placed on the roadway and puncture the tires of a fleeing vehicle, sometimes referred to as spike strips.

Vehicle pursuit - An attempt by one or more law enforcement officers to apprehend a suspect in a motor vehicle who, having been given a visual and audible signal to stop, fails to yield or uses high-speed driving or other evasive tactics (e.g., driving off a highway, turning suddenly) in an attempt to avoid arrest.

344.2 POLICY

It is the policy of this [department/office] to balance the need to apprehend a fleeing suspect with the risks associated with vehicle pursuits.

344.3 INITIATING A PURSUIT

Officers who have received appropriate training are authorized to initiate a vehicle pursuit when the need to apprehend a fleeing suspect clearly outweighs the risks a vehicle pursuit poses for officers and the public.

When balancing the risk of a pursuit with the need to apprehend the suspect, officers shall consider (UAC R728-503-4):

- (a) The seriousness of the known or reasonably suspected crime committed by the suspect and the threat to the safety of the public if the suspect remains at large.
- (b) Whether the identity of the suspect is known with enough certainty to enable apprehension at a later time.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Pursuits

- (c) The speed of the vehicles relative to the conditions of the area, such as the population density, amount of vehicular and pedestrian traffic (e.g., school zones), time of day, and road and weather conditions.
- (d) The pursuing officer's driving capabilities, familiarity with the area, and quality of radio communications with the dispatcher/supervisor.
- (e) The nature of the pursuing unit (e.g., marked vs. unmarked) and its speed and performance capabilities in relation to the fleeing vehicle (e.g., performance motorcycle).
- (f) Whether there are other persons in or on the fleeing vehicle and their relationship to the situation (e.g., passengers, co-offenders, hostages).
- (g) Whether the pursuing unit is carrying passengers other than on-duty police officers. Pursuits should not be undertaken with an arrestee in the pursuit vehicle unless exigent circumstances exist.
- (h) The availability of other resources such as air support or vehicle locator/deactivation technology.
- (i) The likelihood of a pursuit resulting in apprehension.

344.4 PURSUIT UNITS

Vehicle pursuits should be limited to three police [department/office] emergency vehicles (two pursuit units and the supervisor vehicle). However, an officer or supervisor may request that additional units join a pursuit if, after assessing the factors outlined above, it reasonably appears that the number of officers involved may be insufficient to safely arrest the number of suspects (UAC R728-503-5).

344.4.1 EMERGENCY EQUIPMENT

Vehicle pursuits shall only be conducted using authorized police [department/office] vehicles that are equipped with emergency lighting and sirens as required by law. Each pursuit unit's emergency lights and sirens shall remain activated throughout the unit's participation in the pursuit (Utah Code 41-6a-212; UAC R728-503-5).

Officers operating vehicles not equipped with emergency lights and siren are prohibited from pursuing a fleeing vehicle or joining a pursuit. Officers in such vehicles may provide support to pursuing units when needed, but should operate the vehicle in compliance with all traffic laws and should discontinue such support immediately upon arrival of a sufficient number of authorized emergency vehicles or any air support.

344.4.2 MOTORCYCLES AND UNMARKED UNITS

When involved in a pursuit, police [department/office] motorcycles and unmarked vehicles should be replaced by marked four-wheel emergency vehicles as soon as practicable (UAC R728-503-7).

344.4.3 PRIMARY UNIT

The initial pursuing officer should be designated as the primary unit and will be responsible for the conduct of the pursuit unless that unit is unable to remain reasonably close to the suspect's

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Pursuits

vehicle. The primary responsibility of the officer initiating the pursuit is the apprehension of the suspect without unreasonable danger to themselves or others.

As soon as practicable, the primary unit should notify Dispatch of the pursuit, request priority radio traffic, and provide appropriate information including (UAC R728-503-5):

- (a) The location, direction of travel, and estimated speed of the pursuit.
- (b) The description of the fleeing vehicle, including the license plate number, if known.
- (c) The reason for the pursuit.
- (d) A description of the fleeing vehicle's evasive driving behavior (e.g., rapid lane changes, no headlights, driving on the wrong side of the road).
- (e) Known or suspected weapons, threat of force, violence, injuries, hostages, or other unusual hazards.
- (f) The suspected number of occupants and their identities or descriptions.
- (g) The weather, road, and traffic conditions.
- (h) The need for any additional resources or equipment.
- (i) The identities of other law enforcement agencies involved in the pursuit.

The primary unit is responsible for broadcasting the progress of the pursuit until a secondary or air unit joins the pursuit. Once an additional unit joins the pursuit, the primary unit should relinquish the responsibility of broadcasting the progress to the secondary or air unit unless circumstances reasonably indicate otherwise.

344.4.4 SECONDARY UNIT

The second officer in the pursuit should be designated as the secondary unit and is responsible for:

- (a) Notifying Dispatch of their entry into the pursuit.
- (b) Broadcasting the progress of the pursuit, updating known or critical information, and providing changes in the pursuit, unless the situation indicates otherwise.
- (c) Identifying the need for and requesting additional resources or equipment as appropriate.
- (d) Serving as backup to the primary unit once the fleeing vehicle has been stopped.

344.4.5 AIR UNITS

When available, air unit assistance should be requested. The air unit should assume responsibility of broadcasting the pursuit once they have established visual contact with the fleeing vehicle. Ground units should maintain operational control and consider whether the continued close proximity and/or involvement in the pursuit is warranted.

The air unit should coordinate the activities of resources on the ground, report progress of the pursuit, and provide pursuing units with details of upcoming traffic congestion, road hazards, or other information pertinent to evaluating whether to continue the pursuit. If ground units are not

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Pursuits

within visual contact of the fleeing vehicle and the air unit determines that it is unsafe to continue the pursuit, the air unit should recommend termination.

344.5 PURSUIT DRIVING

The decision to use specific driving tactics requires consideration of the same factors as initiating a pursuit. In addition, officers involved in the pursuit should adhere to the following:

- (a) Pursuing units should space themselves far enough from other involved vehicles to be able to see and avoid hazards and react safely to maneuvers by the fleeing vehicle.
- (b) Pursuing units should exercise caution and slow down as necessary when proceeding through intersections.
- (c) Pursuing units should not follow a fleeing vehicle driving against traffic (wrong way) and should instead:
 - 1. Request assistance from available air support.
 - 2. Maintain visual contact with the fleeing vehicle by paralleling it on the correct side of the roadway.
 - 3. Request other units to observe exits available to the fleeing vehicle.
- (d) Pursuing units should request that Dispatch notify the Utah Department of Public Safety and/or another law enforcement agency if it appears that the pursuit may enter its jurisdiction.
- (e) Pursuing units should not attempt to pass other pursuit units unless the situation indicates otherwise or they are requested to do so. Passing another pursuit unit should only be attempted with a clear understanding of the maneuver.

344.5.1 RULES OF THE ROAD

Officers shall drive with due regard for the safety of all persons and property. However, when in pursuit, if there is no unreasonable risk to persons and property, officers may (Utah Code 41-6a-212):

- (a) Proceed past a red or stop signal or stop sign but only after slowing down as may be necessary for safe operation.
- (b) Exceed the speed limit.
- (c) Disregard regulations governing direction of movement or turning in specified directions.

344.5.2 OFFICERS NOT INVOLVED IN THE PURSUIT

Officers not directly involved in the pursuit should stay alert to its progress and location and may proceed safely to intersections ahead of the pursuit to warn cross traffic. When clearing intersections along the pursuit path, officers are authorized to use emergency equipment and should attempt to place their vehicles in locations that provide some safety or an escape route in the event of an unintended collision or a suspect intentionally trying to ram the police [department/office] vehicle.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Pursuits

Other than clearing intersections along the pursuit path, uninvolved officers should avoid operating under emergency conditions (emergency lights and siren) and should remain in their assigned areas unless directed otherwise by a supervisor.

When needed, non-pursuing officers and officers who have dropped out of the pursuit should respond to the pursuit termination point in a non-emergency manner, observing the rules of the road. Officers should not parallel the pursuit route (UAC R728-503-7).

344.6 SUPERVISORY CONTROL AND RESPONSIBILITIES

The field supervisor of the officer initiating the pursuit, or if unavailable, the nearest field supervisor will be responsible for (UAC R728-503-6):

- (a) Immediately notifying the involved units and the dispatcher of supervisory presence and ascertaining all reasonably available information in order to continuously assess the situation and risk factors associated with the pursuit.
- (b) Exercising management and control of the pursuit. However, if practicable, the supervisor shall not be engaged in the pursuit itself.
- (c) Confirming that no more pursuing units than required are involved in the pursuit.
- (d) Directing that the pursuit be terminated if, in the supervisor's judgment, continuing the pursuit is not justified under the guidelines of this policy.
- (e) Assessing the emotional state of the officers involved and directing an officer to disengage from the pursuit if it appears they are unable to control their emotions.
- (f) Requesting additional assistance from air support, canines, or other resources, if available and appropriate.
- (g) Verifying that the proper radio channel is being used.
- (h) Confirming the Watch Commander has been notified of the pursuit.
- (i) Overseeing the notification and/or coordination of outside agencies if the pursuit leaves or is likely to leave the jurisdiction of this [department/office].
- (j) Continuing the management and control of South Salt Lake Police Department units when a pursuit enters another jurisdiction.
- (k) Preparing documentation of the pursuit and conducting a post-pursuit review, as required.

344.6.1 WATCH COMMANDERS RESPONSIBILITIES

Upon becoming aware that a pursuit has been initiated, the Watch Commander should monitor and continually assess the situation and ensure the pursuit is conducted within the guidelines and requirements of this policy. The Watch Commander has the final responsibility for the coordination, control, and termination of a vehicle pursuit and shall be in overall command.

344.7 DISPATCH

Radio communications during a pursuit should be conducted on the primary channel unless instructed otherwise by a supervisor or dispatcher. If the pursuit leaves the jurisdiction of this

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Pursuits

[department/office] or such is imminent, involved units should, whenever available, switch radio communications to a tactical or emergency channel most accessible by participating agencies.

344.7.1 DISPATCH RESPONSIBILITIES

Upon notification or becoming aware that a pursuit has been initiated, the dispatcher is responsible for (UAC R728-503-5):

- (a) Clearing the radio channel of non-emergency traffic.
- (b) Coordinating pursuit communications of the involved units and personnel.
- (c) Broadcasting pursuit updates as well as other pertinent information as necessary.
- (d) Ensuring that a field supervisor is notified of the pursuit.
- (e) Notifying and coordinating with other involved or affected agencies as practicable.
- (f) Notifying the Watch Commander as soon as practicable.
- (g) Assigning an incident number and logging all pursuit activities.

344.8 INTERJURISDICTIONAL CONSIDERATIONS

Unless entry into another jurisdiction is expected to be brief, the primary unit or supervisor should ensure that notification is provided to each outside jurisdiction into which the pursuit is reasonably expected to enter, regardless of whether such jurisdiction is expected to assist (UAC R728-503-6).

344.8.1 ASSUMPTION OF PURSUIT BY ANOTHER AGENCY

When a pursuit enters another agency's jurisdiction, the primary unit or the supervisor should determine whether to request the other agency assume the pursuit, taking into consideration the distance traveled, familiarity with the area, and other pertinent facts.

Once another agency has agreed to assume the pursuit, pursuing units should relinquish control and discontinue participation unless the continued assistance of the South Salt Lake Police Department is requested by the agency assuming the pursuit. Upon relinquishing control of the pursuit, the involved officers may, with supervisory approval, proceed to the termination point in order to provide information and assistance for the arrest of the suspect and reporting of the incident. The supervisor should coordinate such assistance with the assuming agency and obtain any information that is necessary for [department/office] reports.

344.8.2 PURSUITS EXTENDING INTO THIS JURISDICTION

Officers from this [department/office] should not join a pursuit being conducted by another agency unless specifically requested to do so by that agency and with approval from a supervisor.

When a request is made for this [department/office] to assist or take over a pursuit that has entered the jurisdiction of the South Salt Lake Police Department, the Watch Commander or supervisor should review the request as soon as practicable, taking into consideration:

- (a) Whether the need to apprehend the fleeing suspect outweighs the risks of the pursuit to officers and the public.
- (b) Whether there is adequate staffing to continue the pursuit.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Pursuits

- (c) The available units' capabilities to maintain the pursuit.
- (d) The number of available units and other resources of the pursuing agency.

Assistance to a pursuing agency by officers of this [department/office] should terminate at the City limits, provided that the pursuing agency has sufficient assistance from other sources. Ongoing participation from this [department/office] should continue only until sufficient assistance is present.

In the event that a pursuit from another agency terminates within this jurisdiction, officers should provide appropriate assistance to the pursuing agency such as scene control, inter-agency coordination, completion of supplemental reports, and any other reasonable assistance requested or needed.

344.9 PURSUIT INTERVENTION

Pursuit interventions should only be used when it reasonably appears that using the intervention will contain or prevent the pursuit, and the need to immediately stop the fleeing vehicle outweighs the risks of injury or death to officers and others (UAC R728-503-7).

Pursuit interventions may be construed as a use of force, including deadly force, and are subject to the policies guiding such use. Officers should consider the guidelines for the use of force when deciding how, when, where, and if a pursuit intervention should be employed. Refer to the Use of Force Policy for additional guidance.

Whenever practicable, an officer should seek approval from a supervisor before employing any pursuit intervention to stop a fleeing vehicle. Officers should not attempt a pursuit intervention unless they have received the appropriate training for the intervention being used.

344.9.1 TIRE DEFLATION DEVICE

Before deploying a tire deflation device, officers should consider factors such as:

- (a) Speed of the fleeing vehicle - Traveling at high speeds increases the risk the suspect will lose control of the vehicle after driving over or swerving to avoid a tire deflation device.
- (b) Weather and visibility - Tire deflation devices should only be deployed when the location, weather, and other conditions allow the deploying officer to clearly see the fleeing vehicle, pursuit units, and other approaching traffic.
- (c) Cover - Deployment should occur in a location that provides the deploying officer adequate cover and escape from intentional or unintentional exposure to the approaching vehicles.
- (d) Road conditions - Soft or loose material such as dirt or gravel may prevent a tire deflation device from puncturing the vehicle's tire. Deploying the device on loose pavement or icy or wet roads increases the risk of the suspect losing control of the vehicle.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Pursuits

- (e) Characteristics of the deployment area - A tire deflation device should not be deployed in areas that are heavily populated with pedestrians, at times of heavy traffic, or at a location where there is a heightened chance of striking a fixed object.
- (f) Characteristics of the fleeing vehicle - Except in extraordinary circumstances, a tire deflation device should not be used when the fleeing vehicle is a motorcycle or other vehicle with fewer than four wheels, an ATV, a vehicle transporting hazardous materials, or a school bus transporting children.

Because of the risks to deploying officers, the intent to deploy a tire deflation device and its location should be clearly communicated to the dispatcher and all involved units.

344.9.2 PIT

A PIT should only be attempted in a vehicle with a reinforced bumper.

Before conducting a PIT, officers should consider factors such as:

- (a) Speed of the fleeing vehicle - Conducting a PIT while traveling at high speeds increases the risk of the suspect or officer losing control of their vehicle. A PIT should not be conducted at speeds greater than the speed at which the officer has received training.
- (b) Road conditions - Because the intention of a PIT is to cause the fleeing vehicle to spin out by reducing the friction between the tires and the roadway, the material of the roadway (e.g., pavement, gravel, dirt) should be considered and a PIT should not be attempted when road conditions are wet or icy.
- (c) Characteristics of the deployment area - A PIT should not be attempted in areas that are heavily populated with pedestrians, at times of heavy traffic, or at a location where there is a heightened chance of striking a fixed object.
- (d) Characteristics of the fleeing vehicle - A PIT should not be used when the pursued vehicle is a motorcycle or other vehicle with fewer than four wheels, an ATV, a vehicle transporting hazardous materials, or a school bus transporting children. The increased risk of rolling over should be evaluated on vehicles with a high center of gravity.
- (e) Number of pursuit units - A PIT should not be used unless there is a sufficient number of pursuit units available to prevent further movement of the fleeing vehicle after spinning out.

344.9.3 BOXING-IN

Boxing-in should only be used when the fleeing vehicle is stopped or traveling at a low speed.

Boxing-in requires the participation of multiple units and therefore must be carefully coordinated with all involved.

344.9.4 RAMMING AND ROADBLOCKS

Ramming and roadblocks shall only be used when deadly force is warranted and all other reasonable alternatives have been exhausted or reasonably appear ineffective. Roadblocks shall be created in accordance with UAC R728-503-7.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Pursuits

344.9.5 FIREARMS

Specific guidance on the use of a firearm during a vehicle pursuit is addressed in the Use of Force Policy (UAC R728-503-7).

344.10 TERMINATING A PURSUIT

The factors considered when initiating a pursuit should be continually re-evaluated by pursuing units during the pursuit, as the circumstances and conditions change, and as new information becomes available. If at any time the risk of continuing the pursuit outweighs the need to immediately apprehend the suspect, the pursuit should be terminated.

Utah Administrative Code (UAC) R728-503-9

(1) The supervisor or the primary unit in absence of a supervisor shall continually re-evaluate the balance test to assess the pursuit situation.

(a) The supervisor may order the termination of a pursuit at any time.

(b) The primary unit may terminate the pursuit at any time.

(2) A pursuit may be terminated under the following conditions:

(a) the suspect's identity has been determined and future apprehension is likely;

(b) air support is available to track the suspect;

(c) weather or traffic conditions substantially increase the danger of the pursuit beyond the necessity of apprehending the suspect;

(d) the distance between the suspect and pursuing vehicles makes further pursuit futile;

(e) immediate apprehension is not necessary to protect the public or law enforcement officers;

(f) the law enforcement officer is unfamiliar with the area and is unable to accurately communicate location and direction of pursuit; and

(g) the pursuit proceeds the wrong way on a limited access road, for example an interstate highway.

(3) Termination of pursuit shall include deactivating the audible siren and visual light equipment, pulling the vehicle to the side of the road, and stopping.

In addition, a pursuit should be terminated when::

(a) A supervisor directs the pursuit to be terminated.

(b) The location of the fleeing vehicle is no longer known.

(c) The distance between the pursuing units and the fleeing vehicle is so great that further pursuit would be futile or would continue for an unreasonable time and/or distance.

(d) The pursuing unit sustains damage or a mechanical failure that makes it unsafe to drive or renders the emergency lighting and sirens partially or completely inoperable and there are no additional units readily available to take over the pursuit.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Pursuits

When a pursuit terminates for any reason, all pursuit units shall verbally acknowledge termination over the radio, turn off emergency lights and sirens, pull vehicle to the side of the road and stop. r. The primary unit should communicate the location of pursuit termination to the dispatcher.

344.10.1 LOSS OF PURSUED VEHICLE

When a pursuit is terminated because the location of the fleeing vehicle is no longer known, the primary unit should broadcast pertinent information for other units to assist in locating the suspect. The primary unit or supervisor will be responsible for coordinating any further search for the pursued vehicle.

344.10.2 APPREHENSION OF SUSPECTS

Officers should exercise proper self-discipline and sound professional judgment at the conclusion of a pursuit and while apprehending the suspect.

Unless otherwise directed by a supervisor, an officer other than the primary unit should coordinate efforts to apprehend the suspect following the pursuit.

Any use of force necessary to apprehend the suspect shall be consistent with the Use of Force Policy.

344.11 DEBRIEFING

Participating officers should return to the [Department/Office] as soon as practical following a pursuit to debrief with a supervisor.

344.12 REPORTING REQUIREMENTS

Appropriate reports should be completed as required by applicable laws, policies, and procedures.

- (a) Pursuing officers should complete appropriate crime/arrest and pursuit reports.
- (b) The involved supervisor, or if unavailable, the on-duty field supervisor, shall obtain available information and promptly complete appropriate written notification to the Chief of Police or the authorized designee. The notification should briefly summarize the pursuit and include, at a minimum:
 - 1. Date and time of the pursuit.
 - 2. Reason and circumstances surrounding the pursuit (e.g., seriousness of the crime, road and traffic conditions, speed and driving behavior of the fleeing vehicle) that warranted initiation and continuation of the pursuit.
 - 3. Length of pursuit in distance and time, including the starting and termination points.
 - 4. Involved vehicles and officers.
 - 5. Alleged offenses.
 - 6. Whether a suspect was apprehended, as well as the means and methods used.
 - 7. Arrestee information, if applicable.
 - 8. Any injuries and/or medical treatment.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Pursuits

9. Any property or equipment damage.
10. Name of supervisor at the scene or who handled the incident.

After receiving copies of the written notification, reports, and other pertinent information, the Chief of Police or the authorized designee shall conduct or assign a post-pursuit review, as appropriate.

The Chief of Police should direct an annual documented review and analysis of [department/office] vehicle pursuits to minimally include policy suitability, policy compliance, and training or equipment needs. The review should not contain the names of officers, suspects, or case numbers.

344.12.1 CHIEF OF POLICE REVIEW

The Chief of Police shall review each pursuit that results in injury or property damage and determine whether involved members complied with department policies. The Chief of Police shall document and appropriately remedy any policy violations through the disciplinary process (Utah Code 41-6a-212).

344.13 PURSUIT TRAINING

The Training Coordinator should ensure that members of this department receive initial and annual training on vehicle pursuits relevant to their role (e.g., officers, supervisors, air units, dispatchers) (UAC 728-503-10).

Officer training should address decision-making involved in initiating, continuing, and terminating a pursuit by balancing the need to apprehend the suspect with the risk of a pursuit. Subject to available resources, training on pursuit driving and the deployment of pursuit intervention tactics should include scenario-based training and behind-the-wheel practice, in addition to classroom instruction.

344.13.1 POLICY TRAINING REQUIREMENTS

Annual training shall include a review of case law and the [department/office]'s policy and procedure for vehicle pursuits to ensure officers are knowledgeable regarding this policy (UAC R728-503-10).

Service Animals

345.1 PURPOSE AND SCOPE

The purpose of this policy is to provide the guidelines necessary to ensure that the rights of individuals who use service animals to assist with disabilities are protected in accordance with Title II of the Americans with Disabilities Act (ADA).

345.1.1 DEFINITIONS

Definitions related to this policy include:

Service animal - A dog that is trained to do work or perform tasks for the benefit of an individual with a disability, including a physical, sensory, psychiatric, intellectual, or other mental disability. The work or tasks performed by a service animal must be directly related to the individual's disability (28 CFR 35.104).

Service animal also includes a miniature horse if the horse is trained to do work or perform tasks for people with disabilities, provided the horse is housebroken, is under the handler's control, the facility can accommodate the horse's type, size, and weight, and the horse's presence will not compromise legitimate safety requirements necessary for safe operation of the facility (28 CFR 35.136(i)).

All references to "service animals" in this policy include a dog undergoing training to become a service animal (Utah Code 26B-6-801).

345.2 POLICY

It is the policy of the South Salt Lake Police Department to provide equal access to services, programs, and activities of the [Department/Office] to persons with service animals. [Department/Office] members shall protect the rights of persons assisted by service animals in accordance with state and federal law.

345.3 IDENTIFICATION AND USE OF SERVICE ANIMALS

Service animals that are assisting individuals with disabilities are permitted in all public facilities and areas where the general public is allowed. [Department/Office] members are expected to treat individuals with service animals with the same courtesy and respect that the South Salt Lake Police Department affords to all members of the public (28 CFR 35.136; Utah Code 26B-6-803).

Some service animals may be readily identifiable. However, many do not have a distinctive symbol, harness, or collar.

Service animals may be used in a number of ways to provide assistance, including:

- Guiding people who are blind or have low vision.
- Alerting people who are deaf or hard of hearing.
- Retrieving or picking up items, opening doors, or flipping switches for people who have limited use of their hands, arms, or legs.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Service Animals

- Pulling wheelchairs.
- Providing physical support and assisting with stability and balance.
- Doing work or performing tasks for persons with traumatic brain injury, intellectual disabilities, or psychiatric disabilities, such as reminding a person with depression to take medication.
- Alerting a person with anxiety to the onset of panic attacks, providing tactile stimulation to calm a person with post-traumatic stress disorder, assisting people with schizophrenia to distinguish between hallucinations and reality, and helping people with traumatic brain injury to locate misplaced items or follow daily routines.

345.4 INQUIRIES REGARDING SERVICE ANIMALS

If it is apparent or if a member is aware that an animal is a service animal, the individual generally should not be asked any questions as to the status of the animal. If it is unclear whether an animal meets the definition of a service animal, the member should ask the individual only the following questions (28 CFR 35.136(f)):

- Is the animal required because of a disability?
- What task or service has the service animal been trained to perform?

If the individual explains that the animal is required because of a disability and has been trained to work or perform at least one task, the animal meets the definition of a service animal and no further questions as to the animal's status should be asked. The individual should not be questioned about their disabilities nor should members ask any individual to provide any license, certification, or identification card for the service animal.

345.5 CONTACT WITH SERVICE ANIMALS

Service animals are not pets. [Department/Office] members should not interfere with a service animal by talking to, petting, or otherwise initiating contact.

345.6 REMOVAL OF SERVICE ANIMALS

If a service animal is not housebroken, exhibits vicious behavior, poses a direct threat to the health of others, or unreasonably disrupts or interferes with normal business operations, a [department/office] supervisor may direct the handler to remove the animal from the premises. Barking alone is not a threat nor does a direct threat exist if the person takes prompt, effective action to control the service animal (28 CFR 35.136 (b); 28 CFR 35.139).

Each incident must be considered individually, and past incidents alone are not cause for excluding a service animal. Removal of a service animal may not be used as a reason to refuse access to services, programs, and activities to an individual with a disability. Members are expected to provide all services, programs, and activities that are reasonably available to an individual with a disability, with or without a service animal.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Service Animals

345.7 COMPLAINTS

When handling calls of a complaint regarding a service animal, members should remain neutral and should be prepared to explain the ADA requirements concerning service animals to the concerned parties. Businesses are required to allow service animals to accompany their handlers into the same areas that other customers or members of the public are allowed (28 CFR 36.302).

Absent a violation of law independent of the ADA, officers should take no enforcement action beyond keeping the peace. Individuals who believe they have been discriminated against as a result of a disability should be referred to the Civil Rights Division of the U.S. Department of Justice (DOJ).

Chapter 4 - Patrol Operations

Patrol Function

400.1 PURPOSE AND SCOPE

The purpose of this policy is to define the functions of the Patrol Division of the Department to ensure intra-department cooperation and information sharing.

400.1.1 FUNCTION

Officers will generally patrol in clearly marked vehicles, patrol assigned jurisdictional areas of South Salt Lake, respond to calls for assistance, act as a deterrent to crime, enforce state and local laws and respond to emergencies 24 hours per day seven days per week.

Patrol will generally provide the following services within the limits of available resources:

- (a) Patrol that is directed at the prevention of criminal acts, traffic violations and collisions, the maintenance of public order, and the discovery of hazardous situations or conditions.
- (b) Crime prevention activities such as residential inspections, business inspections, community presentations.
- (c) Calls for service, both routine and emergency in nature.
- (d) Investigation of both criminal and non-criminal acts.
- (e) The apprehension of criminal offenders.
- (f) Community Oriented Policing and problem solving activities such as citizen assists and individual citizen contacts of a positive nature.
- (g) The sharing of information between the Patrol Division and other divisions within the Department, as well as other outside governmental agencies.
- (h) The application of resources to specific problems or situations within the community, which may be improved or resolved by Community Oriented Policing and problem solving strategies.
- (i) Traffic direction and control.

400.1.2 TERRORISM

It is the goal of the South Salt Lake Police Department to make every reasonable effort to accurately and appropriately gather and report any information that may relate to either foreign or domestic terrorism. Officers should advise a supervisor as soon as practicable of any activity believed to be terrorism related and should document such incidents with a written report or Field Interview (FI). The supervisor should ensure that all terrorism related reports and FIs are forwarded to the Investigations Division Supervisor in a timely fashion.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Patrol Function

400.2 PATROL INFORMATION SHARING PROCEDURES

The following guidelines are intended to develop and maintain intra-department cooperation and information flow between the various divisions of the South Salt Lake Police Department.

400.2.1 CRIME ANALYSIS UNIT

The Crime Analysis Unit (CAU) will be the central unit for information exchange. Criminal information and intelligence reports can be submitted to the Records Section for distribution to all divisions within the Department through daily and special bulletins.

400.2.2 CRIME REPORTS

A crime report may be completed by any patrol officer who receives criminal information. The report will be processed and forwarded to the appropriate division for retention or follow-up investigation.

400.2.3 PATROL BRIEFING

Patrol supervisors, detective sergeants and special unit sergeants are encouraged to share information as much as possible. All supervisors and/or officers will be provided an opportunity to share information at the daily patrol Briefing as time permits.

400.2.4 INFORMATION CLIPBOARDS

Several information clipboards will be maintained in the Briefing Room and will be available for review by officers from all divisions within the Department. These will include, but not be limited to, the patrol check clipboard, the wanted persons clipboard and the written directive clipboard.

400.2.5 BULLETIN BOARDS

A bulletin board will be kept in the Briefing Room and the Investigations Division for display of suspect information, intelligence reports and photographs. New General Orders will be made available for patrol supervisors and will be discussed at Briefing and shift meetings. A copy of the General Order will be placed on the Briefing Room clipboard.

400.3 CROWDS, EVENTS AND GATHERINGS

Officers may encounter gatherings of people, including but not limited to, civil demonstrations, civic, social and business events, public displays, parades and sporting events. Officers should monitor such events as time permits in an effort to keep the peace and protect the safety and rights of those present. A patrol supervisor should be notified when it becomes reasonably foreseeable that such an event may require increased monitoring, contact or intervention.

Officers responding to an event or gathering that warrants law enforcement involvement should carefully balance the speech and association rights of those present with applicable public safety concerns before taking enforcement action. Officers are encouraged to contact organizers or responsible persons to seek voluntary compliance that may address relevant public safety/order concerns.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Patrol Function

Officers should consider enforcement of applicable state and local laws, when the activity blocks the entrance or egress of a facility or location and when voluntary compliance with the law is not achieved.

Briefing

401.1 PURPOSE AND SCOPE

This policy discusses the activity of [briefing] and includes the tasks that should be accomplished during this short period.

401.2 PREPARATION OF MATERIALS

The supervisor conducting [briefing] is responsible for preparation of the materials necessary for a constructive [briefing]. Supervisors may delegate this responsibility to a subordinate officer in the supervisor's absence or for training purposes.

401.3 POLICY

Briefing is intended to facilitate the accurate flow of information in order to enhance coordination of activities, improve performance and safety, and outline the expected actions of members.

401.4 BRIEFING

All divisions and specialized units will conduct regular [briefing] to discuss, disseminate, and exchange information among [department/office] members, work groups, and other organizations. A supervisor generally will conduct [briefing]. However, the supervisor may delegate this responsibility to a subordinate member in the supervisor's absence or for training purposes.

Briefing should include but is not limited to:

- (a) Providing members with information regarding daily activities, with particular attention given to changes in the status of:
 - 1. Wanted persons.
 - 2. Crime patterns.
 - 3. Suspect descriptions.
 - 4. Intelligence reports and photographs.
 - 5. Community issues affecting law enforcement.
 - 6. Major investigations.
- (b) Notifying members of changes in schedules and assignments.
- (c) Reviewing recent incidents for situational awareness and training purposes.
- (d) Providing training on a variety of subjects.
- (e) Conducting periodic personnel inspections.

Supervisors should also ensure that all members are informed about [departmentalDirective]s and any recent policy changes.

401.4.1 RETENTION OF BRIEFING TRAINING RECORDS

Briefing training materials and a curriculum or summary shall be forwarded to the Training Coordinator for inclusion in training records, as appropriate.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Briefing

401.5 TRAINING

Briefing training should incorporate short segments on a variety of subjects or topics and may include:

- (a) Review and discussion of new or updated policies.
- (b) Presentation and discussion of the proper application of existing policy to routine daily activities.
- (c) Presentation and discussion of the proper application of existing policy to unusual activities.
- (d) Review of recent incidents for training purposes.

Canines

402.1 PURPOSE AND SCOPE

This policy establishes guidelines for the use of canines to augment law enforcement services in the community, including but not limited to locating individuals and contraband and apprehending criminal offenders.

402.2 GUIDELINES FOR THE USE OF CANINES

A canine may be used to locate and apprehend a suspect if the canine handler reasonably believes that the individual has either committed or threatened to commit any serious offense and if any of the following conditions exist:

- (a) There is a reasonable belief that the individual poses an imminent threat of violence or serious harm to the public, any officer or the handler.
- (b) The individual is physically resisting or threatening to resist arrest and the use of a canine reasonably appears to be necessary to overcome such resistance.
- (c) The individual is believed to be concealed in an area where entry by other than the canine would pose a threat to the safety of officers or the public.

It is recognized that situations may arise that do not fall within the provisions set forth in this policy. In any such case, a standard of objective reasonableness shall be used to review the decision to use a canine in view of the totality of the circumstances.

Absent reasonable belief that an individual has committed or threatened to commit a serious offense, mere flight from pursuing officer(s) shall not serve as good cause for the use of a canine to apprehend the individual.

Once the individual has been located and no longer reasonably appears to represent a threat or risk of escape, the canine should be placed in a down-stay or otherwise secured as soon as it becomes reasonably practical.

402.2.1 PREPARATION FOR UTILIZING A CANINE

Prior to the use of a canine to search for or apprehend any individual, the canine handler and/or the supervisor on scene shall carefully consider all pertinent information that is reasonably available at the time. The information should include, but is not limited to the following:

- (a) The individual's age or estimate thereof.
- (b) The nature of the suspected offense.
- (c) Any potential danger to the public and/or other officers at the scene if the canine is released.
- (d) The degree of resistance or threatened resistance, if any, the subject has shown.
- (e) The potential for escape or flight if the canine is not utilized.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Canines

- (f) The potential for injury to officers or the public caused by the suspect if the canine is not utilized.

As circumstances permit, the canine handler should make every reasonable effort to communicate and coordinate with other involved personnel to minimize the risk of unintended injury.

A canine handler shall have the ultimate authority not to deploy the dog. The handler will evaluate each situation and determine if the use of a canine is technically feasible. Generally, the decision to deploy the dog shall remain with the handler. However, a supervisor sufficiently apprised of the situation may decide not to deploy the dog.

402.2.2 WARNINGS GIVEN TO ANNOUNCE THE USE OF A CANINE

Unless it would otherwise increase the risk of injury or escape, two clearly audible warnings to announce that a canine will be released if the person does not come forth shall be made and a reasonable response period provided prior to releasing a canine. The canine handler, when practical, shall first advise the supervisor of his/her decision if a verbal warning is not given prior to releasing the canine. In the event of an apprehension, the handler shall document in any related report whether a verbal warning was given and, if none was given, the reasons why.

402.2.3 USE OF NARCOTIC-DETECTION CANINES

A narcotic-detection trained canine may be used in accordance with current law under the following circumstances:

- (a) To assist in the search for narcotics during a search warrant service.
- (b) To obtain a search warrant by using the detection canine in support of probable cause or in narcotics screening situations.
- (c) To search vehicles, buildings, bags, and any other articles deemed necessary.
- (d) A narcotic-detection canine will not be used to search a person for narcotics.

402.2.4 GUIDELINES FOR NON-APPREHENSION USE

Because canines have senses far superior to those of humans, they may be effectively utilized to track or search for non-criminals (e.g. lost children, individuals who may be disoriented or in need of medical attention) or suspects wanted for minor criminal offenses. In such circumstances, it will be necessary for the handler to evaluate the conditions and the ability of the canine to determine the feasibility of such an application.

- (a) Absent a change in circumstances that present an imminent threat to officers, the canine or the public, such applications should usually be conducted on leash or under such conditions that will minimize the likelihood that the canine will bite or otherwise injure the individual.
- (b) Throughout the deployment of the canine in such circumstances, the handler should consider issuing periodic verbal assurances that the canine will not bite or hurt the person.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Canines

- (c) Unless otherwise directed by a supervisor, assisting personnel should take direction from the handler in order to minimize interference with the canine.
- (d) Once the individual has been located, the canine should be placed in a down-stay or otherwise secured as soon as it becomes reasonably practicable.

402.2.5 REPORTING CANINE USE, BITES AND INJURIES

Whenever the canine is deployed and intentionally bites or otherwise causes injury to a suspect, a supervisor shall be promptly notified and the injuries documented in a Canine Use Report Form. The deployment and injuries should also be included in any related incident or arrest report.

Any unintended bite or injury caused by the canine during deployments, operations, training, presentations or under any other circumstances, either on- or off-duty, shall be promptly reported to the Unit Coordinator. Unintended bites or injuries caused by the canine should be documented in an administrative report, not on a Canine Use Report Form.

402.2.6 REPORTING CANINE INJURIES

In the event that a canine is injured, the injury will be immediately reported to the Watch Commander.

Medical care for any injured canine shall follow the protocol established in the Medical Care of the Canine section of this policy.

The injury will be documented on a Canine Use Report Form.

402.2.7 ASSIGNMENT OF CANINES

Handlers should not transport prisoners in their assigned canine vehicles. If a handler has affected an arrest, a caged patrol unit will be requested to assist in the transportation. Under no circumstances will the handler transport a prisoner that has been bitten by a Police Service Dog.

402.2.8 INTERFERING WITH HANDLER OR CANINE

- (a) Department personnel shall not intentionally or knowingly:
 - 1. Taunt, torment, strike or otherwise assault a police service dog.
 - 2. Throw any object or substance at, or in the path of, a police service dog.
 - 3. Interfere or attempt to interfere with or obstruct a police service dog, or interfere with the handler of the dog in such a manner as to inhibit, restrict, or deprive the handler of his/her control of the dog.
 - 4. Release the dog from its area of control, such as the police vehicle, kennel, or pen, or trespass in that area of control.
 - 5. Place any food, object, or substance into a police service dog's area of control without the permission of the handler.
- (b) Canine handlers and department personnel should be familiar with Utah Code 76-9-306.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Canines

402.3 ASSIGNMENT

Canine teams should be assigned to assist and supplement the Patrol Division to function primarily in assist or cover assignments. However, they may be assigned by the Watch Commander to other functions, such as routine calls for service, based on the current operational needs.

Canine teams should generally not be assigned to handle routine matters that will take them out of service for extended periods of time. If such assignment is necessary, it should only be made with the approval of the Watch Commander.

402.3.1 REQUEST FOR ASSISTANCE FROM OTHER AGENCIES

The Watch Commander or the Unit Coordinator must approve all requests for canine assistance from outside agencies, subject to the following provisions:

- (a) Canine teams shall not be used for any assignment that is not consistent with this policy.
- (b) The handler has the ultimate authority to decide whether the canine should be used for any specific assignment.
- (c) Canine teams shall not be called out while off-duty or used outside the boundaries of the City of South Salt Lake unless authorized by the Watch Commander or the Unit Coordinator.
- (d) It shall be the responsibility of the canine handler to coordinate with outside agency personnel in order to minimize the risk of unintended injury.

402.3.2 REQUEST FOR PUBLIC DEMONSTRATIONS

All public requests for a canine team shall be approved by the Canine Unit Supervisor prior to making any commitment.

Handlers shall not demonstrate any apprehension work to the public unless authorized to do so by the Canine Unit Supervisor.

402.4 CANINE COORDINATOR

The canine coordinator shall be appointed by and directly responsible to the Patrol Division Commander or the authorized designee.

The responsibilities of the coordinator include but are not limited to:

- (a) Reviewing all canine use reports to ensure compliance with policy and to identify training issues and other needs of the program.
- (b) Maintaining a liaison with the vendor kennel.
- (c) Maintaining a liaison with command staff and functional supervisors.
- (d) Maintaining a liaison with other agency canine coordinators.
- (e) Maintaining accurate records to document canine activities.
- (f) Recommending and overseeing the procurement of equipment and services for the teams of handlers and canines.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Canines

- (g) Scheduling all canine-related activities.
- (h) Ensuring the canine teams are scheduled for regular training to maximize their capabilities.

402.4.1 CANINE HANDLER SELECTION

- (a) Handler selection is an important process of ensuring the integrity and working-relations within the Canine Division. All candidates who meet the qualifications will be eligible to participate in the selection process.
- (b) When a position within the Canine unit opens, or a position is being added, department/city policy will be followed when announcing the position.
- (c) All interested candidates will be required to submit a letter interest describing their qualifications, explain why they want to be assigned to the Canine unit and what their goals are for the unit. All letters of interest will be submitted to the unit supervisor.
- (d) Each candidate will be scheduled for an oral interview with the Canine unit supervisor, current canine handlers and a minimum of three outside agency handlers, if available.
 - 1. Candidates will be scored based on the contents of their letter of interest and the oral interview.
 - 2. Candidates will be placed on a list according to scores.
 - 3. Final scores and recommendations will be forwarded to the Chief of Police for final review and approval.

402.4.2 POLICE SERVICE DOG SELECTION

Selecting the proper dog for police service work is critical to the success of the canine program. When selecting a new dog, the obtaining handler and an experienced handler should test the dog. If the obtaining handler is inexperienced, three experienced handlers as well as the obtaining handler should test the dog.

402.5 REQUESTS FOR CANINE TEAMS

Patrol Division members are encouraged to request the use of a canine. Requests for a canine team from [department/office] units outside of the Patrol Division shall be reviewed by the Watch Commander.

402.5.1 OUTSIDE AGENCY REQUEST

All requests for canine assistance from outside agencies must be approved by the Watch Commander and are subject to the following:

- (a) Canine teams shall not be used for any assignment that is not consistent with this policy.
- (b) The canine handler shall have the authority to decline a request for any specific assignment that he/she deems unsuitable.
- (c) Calling out off-duty canine teams is discouraged.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Canines

- (d) It shall be the responsibility of the canine handler to coordinate operations with agency personnel in order to minimize the risk of unintended injury.
- (e) It shall be the responsibility of the canine handler to complete all necessary reports or as directed.

402.5.2 CARE FOR THE CANINE AND EQUIPMENT

The handler shall ultimately be responsible for the health and welfare of the canine and shall ensure that the canine receives proper nutrition, grooming, training, medical care, affection, and living conditions. The handler will be responsible for the following:

- (a) Unless required by a particular application, the handler shall not expose the canine to any foreseeable and unreasonable risk of harm.
- (b) The handler shall maintain all Department equipment under his/her control in a clean and serviceable condition and when not on-duty shall maintain the canine vehicle in a garage (if available), secured from public view.
- (c) When a handler takes a vacation or extended number of days off, the assigned canine vehicle shall be maintained at the Department facility.
- (d) Handlers shall permit the Unit Coordinator to conduct spontaneous on-site inspections of affected areas of their residence as well as the canine vehicle to verify that conditions and equipment conform to this policy.
- (e) Any changes in the living status of the handler which may affect the lodging or environment of the canine shall be reported to the Unit Coordinator as soon as possible.
- (f) When off-duty, canines shall be maintained in kennels, provided by the City, at the homes of their handlers. When a canine is kenneled at the handler's home, the gate shall be secured with a lock. When off-duty, canines may be let out of their kennels while under the direct control of their handlers.
- (g) The canine should be permitted to socialize in the home with the handler's family for short periods of time and under the direct supervision of the handler.
- (h) Under no circumstances will the canine be lodged at another location unless approved by the Unit Coordinator or Watch Commander.
- (i) When off-duty, handlers shall not involve their canines in any activity or conduct unless approved in advance by the Unit Coordinator or Watch Commander.
- (j) Whenever a canine handler anticipates taking a vacation or an extended number of days off, it may be necessary to temporarily relocate the canine. In those situations, the handler shall give reasonable notice to the Unit Coordinator so that appropriate arrangements can be made.

402.5.3 CANINE IN PUBLIC AREAS

All canines shall be kept on a leash when in areas that allow access to the public. Exceptions would include specific police operations for which the canines are trained:

- (a) Canines shall not be left unattended in any area to which the public may have access.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Canines

- (b) When the canine vehicle is left unattended all windows and doors shall be secured in such a manner as to prevent unauthorized access to the dog. The handler shall also ensure that the unattended vehicle remains inhabitable for the canine.

402.5.4 HANDLER COMPENSATION

The canine handler shall be compensated for time spent in the care, feeding, grooming and other needs of the dog as provided in the Fair Labor Standards Act. The compensation shall be prescribed in the Department policy on compensation for employees.

402.6 APPREHENSION GUIDELINES

A canine may be used to locate and apprehend a suspect if the canine handler reasonably believes that the individual has committed, is committing, or is threatening to commit any serious offense and if any of the following conditions exist (UAC R728-507-9):

- (a) There is a reasonable belief the suspect poses an imminent threat of violence or serious harm to the public, any officer, or the handler.
- (b) The suspect is physically resisting or threatening to resist arrest and the use of a canine reasonably appears to be necessary to overcome such resistance.
- (c) The suspect is believed to be concealed in an area where entry by other than the canine would pose a threat to the safety of officers or the public.

It is recognized that situations may arise that do not fall within the provisions set forth in this policy. Such events require consideration of the totality of the circumstances and the use of an objective reasonableness standard applied to the decision to use a canine.

Absent a reasonable belief that a suspect has committed, is committing, or is threatening to commit a serious offense, mere flight from a pursuing officer, without any of the above conditions, shall not serve as the basis for the use of a canine to apprehend a suspect.

Use of a canine to locate and apprehend a suspect wanted for a lesser criminal offense than those identified above requires approval from the Watch Commander. Absent a change in circumstances that presents an imminent threat to officers, the canine, or the public, such canine use should be conducted on-leash or under conditions that minimize the likelihood the canine will bite or otherwise injure the individual.

In all applications, once the suspect has been located and no longer reasonably appears to present a threat or risk of escape, the handler should secure the canine as soon as it becomes reasonably practicable.

If the canine has apprehended the suspect with a secure bite, and the handler believes that the suspect no longer poses a threat, the handler should promptly disengage the canine to release the suspect.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Canines

402.6.1 PREPARATION FOR DEPLOYMENT

Prior to the use of a canine to search for or apprehend any suspect, the canine handler and/or the supervisor on-scene should carefully consider all pertinent information reasonably available at the time. The information should include but is not limited to (UAC R728-507-9):

- (a) The nature and seriousness of the suspected offense.
- (b) Whether violence or weapons were used or are anticipated.
- (c) The degree of resistance or threatened resistance, if any, the suspect has shown.
- (d) The suspect's known or perceived age.
 - 1. A canine shall not be deployed in instances involving a known juvenile suspect unless the juvenile poses an imminent threat of serious bodily injury or death to the officer or another person.
- (e) The potential for injury to officers or the public caused by the suspect if the canine is not utilized.
- (f) Any potential danger to the public and/or other officers at the scene if the canine is released.
- (g) The potential for the suspect to escape or flee if the canine is not utilized.

As circumstances permit, the canine handler should make every reasonable effort to communicate and coordinate with other involved members to minimize the risk of unintended injury.

It is the canine handler's responsibility to evaluate each situation and determine whether the use of a canine is appropriate and reasonable. The canine handler is not permitted to deploy the use of the canine as a pain compliance technique. The canine handler shall have the authority to decline the use of the canine whenever the handler deems deployment is unsuitable.

A supervisor who is sufficiently apprised of the situation may prohibit deploying the canine.

Unless otherwise directed by a supervisor, assisting members should take direction from the handler in order to minimize interference with the canine.

402.6.2 EMERGENCY MEDICAL CARE

The handler shall notify the Unit Coordinator as soon as practicable when emergency medical care is required.

Depending on the severity of the illness or injury, the canine should either be treated by the designated veterinarian or transported to a designated emergency medical facility for treatment. If the handler and dog are out of the area, the handler may use the nearest available veterinarian.

402.7 TRAINING AND CERTIFICATION

Each law enforcement canine handler and canine shall be initially certified and annually recertified by a qualifying canine handler and canine entity in accordance with the Utah POST handler and canine certification standards and the Law Enforcement Canine Team Certification Act.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Canines

402.8 NON-APPREHENSION GUIDELINES

Properly trained canines may be used to track or search for non-criminals (e.g., lost children, individuals who may be disoriented or in need of medical attention). The canine handler is responsible for determining the canine's suitability for such assignments based on the conditions and the particular abilities of the canine. When the canine is deployed in a search or other non-apprehension operation, the following guidelines apply:

- (a) Absent a change in circumstances that presents an imminent threat to officers, the canine, or the public, such applications should be conducted on-leash or under conditions that minimize the likelihood the canine will bite or otherwise injure the individual, if located.
- (b) Unless otherwise directed by a supervisor, assisting members should take direction from the handler in order to minimize interference with the canine.
- (c) Throughout the deployment, the handler should periodically give verbal assurances that the canine will not bite or hurt the individual and encourage the individual to make him/herself known.
- (d) Once the individual has been located, the handler should place the canine in a down-stay or otherwise secure it as soon as reasonably practicable.

402.8.1 CONTINUED TRAINING

Each canine team shall thereafter be recertified to current Utah POST or other recognized and approved certification standards on an annual basis. Additional training considerations are as follows:

- (a) Canine teams shall receive training as defined in the current contract with the department's canine training provider.
- (b) Canine handlers are encouraged to engage in additional training with approval of the Unit Coordinator.
- (c) To ensure that all training is consistent, no handler, trainer or outside vendor is authorized to train to a standard that is contrary to the policies of the South Salt Lake Police Department.
- (d) All canine training shall be conducted while on-duty unless otherwise approved by the Unit Coordinator or Watch Commander.

402.8.2 NARCOTICS DETECTION

A canine trained in narcotics detection may be used in accordance with current law and under certain circumstances, including:

- (a) The search of vehicles, buildings, bags, and other articles.
- (b) Assisting in the search for narcotics during a search warrant service.
- (c) Obtaining a search warrant by using the narcotics-detection trained canine in support of probable cause.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Canines

A narcotics-detection trained canine will not be used to search a person for narcotics unless the canine is trained to passively indicate the presence of narcotics.

402.8.3 BOMB/EXPLOSIVE DETECTION

Because of the high risk of danger to the public and officers when a bomb or other explosive device is suspected, the use of a canine team trained in explosive detection may be considered. When available, an explosive-detection canine team may be used in accordance with current law and under certain circumstances, including:

- (a) Assisting in the search of a building, structure, area, vehicle, or article where an actual or suspected explosive device has been reported or located.
- (b) Assisting with searches at transportation facilities and vehicles (e.g., buses, airplanes, trains).
- (c) Preventive searches at special events, VIP visits, official buildings, and other restricted areas. Searches of individuals should remain minimally intrusive and shall be strictly limited to the purpose of detecting explosives.
- (d) Assisting in the search of scenes where an explosion has occurred and an explosive device or secondary explosive device is suspected.

At no time will an explosive-detection trained canine be used to render a suspected device safe or clear.

402.9 HANDLER SELECTION

The minimum qualifications for the assignment of canine handler include:

- (a) An officer who is currently off probation.
- (b) Residing in an adequately fenced single-family residence (minimum 5-foot-high fence with locking gates).
- (c) A garage that can be secured and can accommodate a canine vehicle.
- (d) Living within 30 minutes travel time from the South Salt Lake City limits.
- (e) Agreeing to be assigned to the position for a minimum of three years.

402.10 HANDLER RESPONSIBILITIES

The canine handler shall ultimately be responsible for the health and welfare of the canine and shall ensure that the canine receives proper nutrition, grooming, training, medical care, affection, and living conditions.

The canine handler will be responsible for the following:

- (a) Except as required during appropriate deployment, the handler shall not expose the canine to any foreseeable and unreasonable risk of harm.
- (b) The handler shall maintain all [department/office] equipment under their control in a clean and serviceable condition.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Canines

- (c) When not in service, the handler shall maintain the canine vehicle in a locked garage, away from public view.
- (d) When a handler is off-duty for an extended number of days, the assigned canine vehicle should be stored at the South Salt Lake Police Department facility.
- (e) Handlers shall permit the canine coordinator to conduct spontaneous on-site inspections of affected areas of their homes as well as their canine vehicles to verify that conditions and equipment conform to this policy.
- (f) Any changes in the living status of the handler that may affect the lodging or environment of the canine shall be reported to the canine coordinator as soon as possible.
- (g) When off-duty, the canine shall be in a kennel provided by the City at the home of the handler. When a canine is kenneled at the handler's home, the gate shall be secured with a lock. When off-duty, the canine may be let out of the kennel while under the direct control of the handler.
- (h) The canine should be permitted to socialize in the home with the handler's family for short periods of time and under the direct supervision of the handler.
- (i) Under no circumstances will the canine be lodged at another location unless approved by the canine coordinator or Watch Commander.
- (j) When off-duty, the handler shall not involve the canine in any law enforcement activity or official conduct unless approved in advance by the canine coordinator or Watch Commander.
- (k) Whenever a canine handler is off-duty for an extended number of days, it may be necessary to temporarily relocate the canine. In those situations, the handler shall give reasonable notice to the canine coordinator so that appropriate arrangements can be made.

402.10.1 CANINE IN PUBLIC AREAS

The canine should be kept on a leash when in areas that allow access to the public. Exceptions to this rule would include specific law enforcement operations for which the canine is trained.

- (a) A canine shall not be left unattended in any area to which the public may have access.
- (b) When the canine vehicle is left unattended, all windows and doors shall be secured in such a manner as to prevent unauthorized access to the canine. The handler shall also ensure that the unattended vehicle remains inhabitable for the canine.

402.10.2 IMMUNITY

All duly authorized peace officers, while providing substance abuse training to law enforcement or the community or while providing canine drug detection training in performance of their official duties, and any person working under their immediate direction, supervision, or instruction are immune from prosecution for narcotics possession (Utah Administrative Code R156-37-305(2)).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Canines

402.10.3 RETIRED POLICE SERVICE CANINE

The Police Service Dog will be retired on the recommendation of the veterinarian, due to the dog's age, or for medical reasons. Police Service Dogs may also be retired for unresolvable performance problems.

- (a) Legal ownership of the Police Service Dog belongs to South Salt Lake City Police Department.
 - 1. When a Police Service Dog reaches retirement, the accepting handler will purchase the dog for the sum of one dollar.
- (b) At the discretion of the canine unit supervisor, the retired dog will be:
 - 1. Sold to the current handler.
 - 2. Sold to the previous handler if the current handler is unable to accept the dog.
 - 3. Euthanized, if no handler can accept the dog.
- (c) Once the PSD has been retired and sold the City of South Salt Lake will no longer be responsible for daily care.
- (d) Upon the PSD's retirement, the department owned "Tuff-Shed" and kennel will be returned to the department for re-assignment.

Crime and Disaster Scene Integrity

403.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance in handling a major crime or disaster.

403.2 CRIME SCENE RESPONSIBILITY

The first officer at the scene of a crime or major incident is generally responsible for the preservation of the scene. Officers shall also consider officer safety and public safety issues, including rendering medical aid to any injured parties. Once an officer has assumed or been assigned to maintain the integrity of the crime/disaster scene it shall be maintained until the officer is relieved by order of a supervisor.

403.2.1 FIRST RESPONDER CONSIDERATIONS

The following list generally describes the first responder's function at a crime or disaster scene. This list is not intended to be all-inclusive, is not necessarily in order and may be altered according to the demands of each situation:

- (a) Ensure no suspects are still in the area.
- (b) Broadcast emergency information including all requests for additional assistance.
- (c) Provide first-aid to injured parties if it can be done safely.
- (d) Secure the inner perimeter with crime scene tape.
- (e) Protect items of apparent evidentiary value.
- (f) Start a chronological log noting critical times and personnel allowed access.

403.2.2 ENFORCEMENT

Any sworn member of the South Salt Lake Police Department may enforce all orders of the local health authority issued for the purpose of preventing the spread of any contagious, infectious or communicable disease (Utah Code 26-6b-2 and Utah Code 26-6b-3).

If an individual refuses to comply with an order of the Department of Health or local health authority issued to prevent the spread of a communicable disease, infectious agent, or contamination, the issuing authority may petition a District Court for an order for involuntary examination, treatment, quarantine or isolation of the individual in accordance with Utah Code 26-6-4.

403.3 SEARCHES AT CRIME OR DISASTER SCENES

Officers arriving at crime or disaster scenes are often faced with the immediate need to search for and render aid to victims and to determine if suspects are present and continue to pose a threat. Once officers are satisfied that no additional suspects are present and/or there are no injured persons to be treated, those exigent circumstances will likely no longer exist. Officers should thereafter secure the scene and conduct no further search until proper authority for the search is obtained.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Crime and Disaster Scene Integrity

403.3.1 CONSENT

Officers should seek consent to search from authorized individuals where possible. However, in the case of serious crimes or major investigations it may be prudent to obtain a search warrant. Consent may be sought even in cases where a search warrant has been granted.

403.4 EXECUTION OF HEALTH ORDERS

Any sworn member of the South Salt Lake Police Department may assist in enforcement of orders of restriction issued by the Department of Health and Human Services or local health authority for the purpose of preventing the spread of any contagious, infectious, or communicable disease (Utah Code 26B-7-304; Utah Code 26B-7-306).

Special Weapons and Tactics Unit (SWAT)

404.1 PURPOSE AND SCOPE

The Special Weapons and Tactics Unit is comprised of two specialized teams: the Crisis Negotiation Team (CNT) and the Special Weapons and Tactics Team (SWAT). The unit has been established to provide specialized support in handling critical field operations where intense negotiations and/or special tactical deployment methods beyond the capacity of field officers appear to be necessary. Both units are merged with Unified Police Department.

404.1.1 OPERATIONAL AND ADMINISTRATIVE STRUCTURE

The Policy Manual sections pertaining to the Crisis Response Unit are divided into Administrative and Operational sections. Since situations that necessitate the need for such a police response vary greatly from incident to incident and such events often demand on-the-scene evaluation, the Operational Policy outlined in this manual section serves as a guideline to Department personnel allowing for appropriate on scene decision making as required. The Administrative Procedures, however, are more restrictive and few exceptions should be taken.

404.1.2 SWAT TEAM DEFINED

A SWAT team is a designated unit of law enforcement officers that is specifically trained and equipped to work as a coordinated team to resolve critical incidents that are so hazardous, complex or unusual that they may exceed the capabilities of first responders or investigative units. These incidents include, but not limited to, hostage taking, barricaded suspects, snipers, terrorist acts and other high-risk incidents. As a matter of Department policy, such a unit may also be used to serve high-risk warrants, both search and arrest, where public and officer safety issues warrant the use of such a unit.

404.2 OPERATION GUIDELINES FOR CRISIS RESPONSE UNIT

Generally, the SWAT Team and the Crisis Negotiation Team will be activated together. It is recognized, however, that a tactical team may be used in a situation not requiring the physical presence of the Crisis Negotiation Team, such as warrant service operations. This shall be at the discretion of the SWAT Team Leader.

404.2.1 ON-SCENE DETERMINATION

The On-Duty Watch Commander or On-Scene Supervisor in charge at the scene of a particular event will assess whether to request the SWAT Team to respond. Upon final determination by the Watch Commander or On-Scene Supervisor, he/she will notify the Deputy Chief of Police for final approval.

404.2.2 APPROPRIATE SITUATIONS FOR USE OF CRISIS RESPONSE UNIT

The following are examples of incidents which may result in the activation of the S.W.A.T. Team:

- (a) Barricaded suspects who refuse an order to surrender.
- (b) Incidents where hostages are taken.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Special Weapons and Tactics Unit (SWAT)

- (c) Cases of suicide threats.
- (d) Arrests of dangerous persons.
- (e) Any situation that could enhance the ability to preserve life, maintain social order and ensure the protection of property.

404.2.3 MOBILIZATION OF CRISIS RESPONSE UNIT

Absent Exigent Circumstances, the On-Scene Supervisor shall make a request to the Watch Commander for the activation of SWAT. The Watch Commander shall then notify the Commander over the SWAT Team. If unavailable, the SWAT Team Leader shall be notified. A current mobilization list shall be maintained by VECC by the SWAT Supervisor. The Watch Commander or On-Scene Supervisor will then notify the Deputy Chief of Police as soon as practical.

The Watch Commander or On-Scene Supervisor should advise the SWAT Supervisor with as much of the following information which is available at the time:

- (a) The number of suspects, known weapons and resources.
- (b) If the suspect is in control of hostages.
- (c) If the suspect is barricaded.
- (d) The type of crime involved.
- (e) If the suspect has threatened or attempted suicide.
- (f) The location of the command post and a safe approach to it.
- (g) The extent of any perimeter and the number of officers involved.
- (h) Any other important facts critical to the immediate situation and whether the suspect has refused an order to surrender.

404.2.4 FIELD UNIT RESPONSIBILITIES

While waiting for the SWAT Team to arrive, field personnel should, if safe, practical and sufficient resources exist:

- (a) Establish an inner and outer perimeter.
- (b) Establish a command post outside of the inner perimeter.
- (c) Evacuate any injured persons or citizens in the zone of danger.
- (d) Attempt to establish preliminary communication with the suspect. Once the SWAT Team has arrived, all negotiations should generally be halted to allow the negotiators and SWAT time to set up.
- (e) Be prepared to brief the SWAT Commander on situation.
- (f) Plan for, and stage, anticipated resources.
- (g) Determine whether a hostage situation does in fact exist.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Special Weapons and Tactics Unit (SWAT)

- (h) Establish incident command and adhere to the principals of incident command.
- (i) Advise dispatch of the nature and extent of the situation.
- (j) Establish a safe assembly point.
- (k) Request that a supervisor respond and brief that supervisor of all known facts.
- (l) Protect the crime scene if the suspect has fled.

404.2.5 INCIDENT COMMAND (INITIAL) RESPONSIBILITY

To maintain the principle of Singularity of Command at the incident scene, all supervisors and support staff such as negotiators, inner and outer perimeter supervisors, SWAT Commander, and Public Information Officer will report directly to the Incident Commander. Senior command level officers and other officials who respond to the incident will also contact the Incident Commander. All information and assistance will be directed to the Incident Commander. The Incident Commander will:

- (a) Establish an inner perimeter to contain the situation. (The inner perimeter should be small enough to severely limit the hostage situation, but large enough to protect the responding members.)
- (b) Establish an outer perimeter. (The outer perimeter will exclude the public, including the media, from the scene. A separate staging area for the media should be established.)
- (c) Assign one member to supervise each perimeter group (inner and outer).
- (d) Establish a command post (CP). The CP should be established within the outer perimeter.
- (e) Evacuate all other persons from the area secured.
- (f) Arrange for necessary support such as fire apparatus, paramedics, ambulances, SWAT, PIO.
- (g) Insure that communication with the suspect has been established.
- (h) Arrange for a Crisis Negotiator.
- (i) Clear a radio frequency for the situation.

404.2.6 OTHER DUTIES AND RESPONSIBILITIES

Sworn members may be assigned to the following functions:

- (a) Operations Officer: Responsible for insuring that all involved personnel, agencies and support units are kept advised of the situation status.
- (b) Recorder: Assigned to note and document all times and activities occurring in the situation. The first member to arrive at the scene remains responsible for the initial report.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Special Weapons and Tactics Unit (SWAT)

404.2.7 NEGOTIATION AND RESOLUTION

Sworn members performing as hostage negotiators (whether specifically trained or not) should take into consideration the basic motivations and tactics used when dealing with the following types of hostage takers.

- (a) Thwarted Criminal: Crimes in progress interrupted when hostages are taken to secure escape are usually dealt with by appealing to rational arguments, emphasizing guarantee of safety, and increased penalty to criminals who harm hostages.
- (b) Mentally Ill: Often irrational and unpredictable. Demands and conversation should be carefully evaluated for clues to the hostage taker's mental condition. Time acts against the hostage taker as emotions take a toll on the physical and mental condition of the hostage taker.
- (c) Terrorist: Usually have an ideological commitment to a cause of some perceived social injustice. Resolve to die for a cause may deteriorate with passage of time. Mistakes should be quickly capitalized on.
- (d) Correctional Facility: Usually attempting to draw attention to perceived problems in the institution or to gain freedom. Swift action to isolate and limit the involvement of other prisoners is essential. Freedom is not a negotiable demand.

404.2.8 NEGOTIATION GUIDELINES

- (a) Acceptable requests and demands should be met only after concessions by the hostage taker.
- (b) No offer or exchange of law enforcement members or civilians for hostages will be made.
- (c) No negotiation will be made to supply the suspect(s) any workable weapons.
- (d) No negotiation will be made to allow suspect(s) to leave the scene with any hostages.
- (e) Time limitations will be acknowledged, but continually delayed.
- (f) An attempt will be made to have the suspect(s) establish personal rapport with the negotiator.
- (g) No major demand will be granted immediately.
- (h) The negotiation will occur from such a place so as to insure that the negotiator does not become a hostage.
- (i) The suspect will be continually reassured that there will be no harm to the hostage taker, if the hostage taker releases the hostages and surrenders.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Special Weapons and Tactics Unit (SWAT)

404.2.9 SWAT ACTIVITIES

If SWAT responds, those sworn members securing the inner perimeter will be relieved by SWAT when they arrive and are so assigned. The SWAT Commander will assume command of all activities inside the inner perimeter and work in coordination with the Incident Commander.

Ride-Along Program

405.1 PURPOSE AND SCOPE

The Ride-Along Program provides an opportunity for community members to experience the law enforcement function firsthand. This policy provides the requirements, approval process and hours of operation for the Ride-Along Program.

405.1.1 POLICY

Only those persons with written authorization from the Chief of Police or his/her designee shall be allowed to participate in the department's citizen ride-along program. Priority shall be given to South Salt Lake Police Officers spouses or significant others.

405.1.2 ELIGIBILITY

(a) Ride-alongs are limited to the following categories:

1. Immediate Family Member of the officer, further defined as spouse, significant other, child, step-child, daughter-in-law, son-in-law, parent, step-parent, grandchild, mother-in-law, father-in-law, sister-in-law, brother-in-law, grandparent, spouse's or significant others grandparent, and brother or sister.
2. Community members currently enrolled and participating in an active Citizen Academy Class are authorized one (1) ride-along.
3. Administrative ride-alongs are persons riding in an official capacity, such as District Attorneys, City officials, Civilian Review Board member, City Council member, Professional Support Staff, and /or approved person by the Deputy Chief or his/her designee.
4. Ride-alongs need to have prior approval by the Deputy Chief or his/her designee.
5. The Deputy Chief or his/her designee will coordinate with the Patrol Watch Commander the date and time of approved ride-a-long.
6. The Chief, or his/her designee may approve a ride-along for individuals with a relevant interest in the operations of the police department.

405.2 COMPLETION OF WAIVER AGREEMENT

All persons participating in a ride-along, shall complete a release of liability waiver prior to actually riding. Upon completion of the ride-along, the original waiver agreement shall be forwarded to the Chief's office for review and tracking.

405.2.1 PROGRAM REQUIREMENTS AND RESTRICTIONS

- (a) Ride-along participants must be at least eighteen (18) years of age or older.
- (b) The Deputy Chief or his/her designee must authorize the ride-along prior to commencement. A Release of Liability Waiver form must be signed and submitted prior to the ride-along.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Ride-Along Program

- (c) Any individual who is a convicted felon, suspected to be involved in criminal activity, under the supervision of Probation and Parole, or has outstanding warrants, will not be allowed to participate in this program.
- (d) Officers are restricted to one (1) ride-along a month.
- (e) Ride-alongs are limited to four (4) hours.
- (f) Audio or visual recording devices owned by the participant are prohibited, unless authorized by the Chief of Police or his/her designee.
- (g) Ride-along participants shall not use tobacco products while inside the police department, inside any department owned vehicle(s), while in view of the public in the presence of an officer, or in any other location where tobacco use is prohibited.
- (h) Ride-along participants shall not smell of, possess, or consume alcoholic beverages during the ride-along.
- (i) South Salt Lake Police officers will not participate in any ride-along program outside of the City of South Salt Lake without prior approval of the Chief of Police or his/her designee.
- (j) The ride-along participant is prohibited from becoming involved in any investigation by touching evidence, handling police equipment, or engaging in conversation with victims, suspects, or witnesses.

405.2.2 SUITABLE ATTIRE

Any person approved to ride-along is required to be suitably dressed in collared shirt, blouse or jacket, slacks and shoes. Sandals, T-shirts, tank tops, shorts and ripped or torn blue jeans are not permitted. Hats and ball caps will not be worn in the police vehicle. The Watch Commander or field supervisor may refuse a ride along to anyone not properly dressed.

405.2.3 PEACE OFFICER RIDE-ALONGS

Off-duty members of the Department or any other law enforcement agency will not be permitted to ride-along with on-duty officers without the expressed consent of the Deputy Chief.. In the event that such a ride-along is permitted, the off-duty employee shall not be considered on-duty and shall not represent themselves as a peace officer or participate in any law enforcement activity except as emergency circumstances may require.

405.2.4 RIDE-ALONG CRIMINAL HISTORY CHECK

All ride-along applicants are subject to a criminal history check. The criminal history check may include a local records check and a state records check through the Bureau of Criminal Investigation (BCI) prior to their approval as a ride-along with a law enforcement officer, provided that the ride-along is not an employee of the South Salt Lake Police Department.

405.3 OFFICER'S RESPONSIBILITY

The officer shall advise the dispatcher that a ride-along is present in the vehicle before going into service. Officers shall consider the safety of the ride-along at all times. Officers should use sound discretion when encountering a potentially dangerous situation, and if feasible, let the participant

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Ride-Along Program

out of the vehicle in a well-lighted place of safety. The dispatcher will be advised of the situation and as soon as practical have another police vehicle respond to pick up the participant at that location. The ride-along may be continued or terminated at this time.

Officers shall not engage in a vehicle pursuit with a ride-along passenger.

405.4 CONTROL OF RIDE-ALONG

The assigned employee shall maintain control over the ride-along at all times and instruct him/her in the conditions that necessarily limit their participation. These instructions should include:

- (a) The ride-along will follow the directions of the officer.
- (b) The ride-along will not become involved in any investigation, handling of evidence, discussions with victims or suspects or handling any police equipment.
- (c) The ride-along may terminate the ride at any time. If the ride-along interferes with the performance of the officer's duties, the officer may terminate the ride-along and return the observer to his/her home or to the station.
- (d) Ride-alongs may be allowed to continue riding during the transportation and booking process provided this does not jeopardize their safety.
- (e) Officers will not allow any ride-alongs to be present in any residence or situation that would jeopardize their safety or cause undue stress or embarrassment to a victim or any other citizen.
- (f) Under no circumstance shall a civilian ride-along be permitted to enter a private residence with an officer without the expressed consent of the resident or other authorized person.

Hazardous Material Response

406.1 PURPOSE AND SCOPE

Exposure to hazardous materials presents potential harm to department members and the public. This policy outlines the responsibilities of members who respond to these events and the factors that should be considered while on-scene, including the reporting of exposures and supervisor responsibilities.

406.1.1 DEFINITIONS

Definitions related to this policy include:

Hazardous material - A substance which by its nature, containment and reactivity, has the capability of inflicting harm during exposure; characterized as being toxic, corrosive, flammable, reactive, an irritant or strong sensitizer and thereby posing a threat to health when improperly managed.

406.2 HAZARDOUS MATERIAL RESPONSE

Members may encounter situations involving suspected hazardous materials, such as at the scene of a traffic collision, chemical spill, or fire. When members come into contact with a suspected hazardous material, they should take certain steps to protect themselves and other persons.

The fire department is the agency trained and equipped to properly respond to and mitigate most incidents involving hazardous materials and biohazards.

Responders should not perform tasks or use equipment without proper training. A responder entering the area may require decontamination before he/she is allowed to leave the scene, and should be evaluated by appropriate technicians and emergency medical services personnel for signs of exposure.

406.3 REPORTING EXPOSURE

Department members who believe they have been exposed to a hazardous material shall immediately report the exposure to a supervisor. Each exposure shall be documented by the member in an incident report that shall be forwarded via chain of command to the Watch Commander as soon as practicable. Should the affected member be unable to document the exposure for any reason, it shall be the responsibility of the notified supervisor to complete the report.

Injury or illness caused or believed to be caused from exposure to hazardous materials shall be reported the same as any other on-duty injury or illness, in addition to a crime report or incident report as applicable.

406.3.1 SUPERVISOR RESPONSIBILITIES

When a supervisor has been informed that a member has been exposed to a hazardous material, he/she shall ensure that immediate medical treatment is obtained and appropriate action is taken to mitigate the exposure or continued exposure.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Hazardous Material Response

To ensure the safety of members, PPE is available from supervisors. PPE not maintained by this department may be available through the appropriate fire department or emergency response team.

406.4 POLICY

It is the policy of the South Salt Lake Police Department to respond to hazardous material emergencies with due regard for the safety of the public and those members responding to such incidents.

406.5 CONSIDERATIONS

The following steps should be considered at any scene involving suspected hazardous materials:

- (a) Make the initial assessment of a potentially hazardous material from a safe distance.
- (b) Notify Dispatch, appropriate supervisors, the appropriate fire department and hazardous response units.
 - 1. Provide weather conditions, wind direction, a suggested safe approach route and any other information pertinent to responder safety.
- (c) Wear personal protective equipment (PPE), being cognizant that some hazardous material can be inhaled.
- (d) Remain upwind, uphill and at a safe distance, maintaining awareness of weather and environmental conditions, until the material is identified and a process for handling has been determined.
- (e) Attempt to identify the type of hazardous material from a safe distance using optical aids (binoculars or spotting scopes) if they are available. Identification can be determined by:
 - 1. Placards or use of an emergency response guidebook.
 - 2. Driver's statements or shipping documents from the person transporting the material.
 - 3. Information obtained from any involved person with knowledge regarding the hazardous material. Information should include:
 - (a) The type of material.
 - (b) How to secure and contain the material.
 - (c) Any other information to protect the safety of those present, the community and the environment.
- (f) Provide first aid to injured parties if it can be done safely and without contamination.
- (g) Make reasonable efforts to secure the scene to prevent access from unauthorized individuals and to protect and identify any evidence.
- (h) Begin evacuation of the immediate and surrounding areas, dependent on the material. Voluntary evacuation should be considered; mandatory evacuation may be necessary and will depend on the type of material.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Hazardous Material Response

- (i) Establish a decontamination area when needed.
- (j) Activate automated community notification systems, if applicable.
- (k) Notify the Utah Department of Environmental Quality, Division of Waste Management and Radiation Control.

Hostage and Barricade Incidents

407.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for situations where officers have legal cause to contact, detain or arrest a person, and the person refuses to submit to the lawful requests of the officers by remaining in a structure or vehicle and/or by taking a hostage.

The scope of this policy is not intended to address all variables that officers encounter during their initial response or when a hostage or barricade situation has developed. This policy does not require or purport to recommend specific strategies or tactics for resolution as each incident is a dynamic and rapidly evolving event.

407.1.1 DEFINITIONS

Definitions related to this policy include:

Barricade situation - An incident where a person maintains a position of cover or concealment and ignores or resists law enforcement personnel, and it is reasonable to believe the subject is armed with a dangerous or deadly weapon.

Hostage situation - An incident where it is reasonable to believe a person is unlawfully held by a hostage-taker as security so that specified terms or conditions will be met.

407.2 POLICY

It is the policy of the South Salt Lake Police Department to address hostage and barricade situations with due regard for the preservation of life and balancing the risk of injury, while obtaining the safe release of hostages, apprehending offenders and securing available evidence.

407.3 COMMUNICATION

When circumstances permit, initial responding officers should try to establish and maintain lines of communication with a barricaded person or hostage-taker. Officers should attempt to identify any additional subjects, inquire about victims and injuries, seek the release of hostages, gather intelligence information, identify time-sensitive demands or conditions and obtain the suspect's surrender.

When available, department-authorized negotiators should respond to the scene as soon as practicable and assume communication responsibilities. Negotiators are permitted to exercise flexibility in each situation based upon their training, the circumstances presented, suspect actions or demands and the available resources.

407.3.1 EMERGENCY COMMUNICATIONS

Should circumstances at the scene permit, a supervisor or negotiator may contact the Attorney General or the District Attorney for approval to intercept any wire, electronic or oral communication and/or to use an eavesdropping device (e.g., camera or audio device) when there is an immediate threat of death or serious bodily injury to any person or to national security. The supervisor or negotiator who has been granted approval shall ensure that an application for an appropriate court

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Hostage and Barricade Incidents

order approving the interception is sought within 48 hours after the interception begins (Utah Code 77-23a-10(7)).

407.4 FIRST RESPONDER CONSIDERATIONS

First responding officers should promptly and carefully evaluate all available information to determine whether an incident involves, or may later develop into, a hostage or barricade situation.

The first responding officer should immediately request a supervisor's response as soon as it is determined that a hostage or barricade situation exists. The first responding officer shall assume the duties of the supervisor until relieved by a supervisor or a more qualified responder. The officer shall continually evaluate the situation, including the level of risk to officers, to the persons involved and to bystanders, and the resources currently available.

The handling officer should brief the arriving supervisor of the incident, including information about suspects and victims, the extent of any injuries, additional resources or equipment that may be needed, and current perimeters and evacuation areas.

407.4.1 BARRICADE SITUATION

Unless circumstances require otherwise, officers handling a barricade situation should attempt to avoid a forceful confrontation in favor of stabilizing the incident by establishing and maintaining lines of communication while awaiting the arrival of specialized personnel and trained negotiators. During the interim the following options, while not all-inclusive or in any particular order, should be considered:

- (a) Ensure injured persons are evacuated from the immediate threat area if it is reasonably safe to do so. Request medical assistance.
- (b) Assign personnel to a contact team to control the subject should he/she attempt to exit the building, structure or vehicle, and attack, use deadly force, attempt to escape or surrender prior to additional resources arriving.
- (c) Request additional personnel, resources and equipment as needed (e.g., canine team, air support).
- (d) Provide responding emergency personnel with a safe arrival route to the location.
- (e) Evacuate non-injured persons in the immediate threat area if it is reasonably safe to do so.
- (f) Attempt or obtain a line of communication and gather as much information on the subject as possible, including weapons, other involved parties, additional hazards or injuries.
- (g) Establish an inner and outer perimeter as circumstances require and resources permit to prevent unauthorized access.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Hostage and Barricade Incidents

- (h) Evacuate bystanders, residents and businesses within the inner and then outer perimeter as appropriate. Check for injuries, the presence of other involved subjects, witnesses, evidence or additional information.
- (i) Determine the need for and notify the appropriate persons within and outside the Department, such as command officers and the Public Information Officer.
- (j) If necessary and available, establish a tactical or exclusive radio frequency for the incident.
- (k) Establish a command post.

407.4.2 HOSTAGE SITUATION

Officers presented with a hostage situation should attempt to avoid a forceful confrontation in favor of controlling the incident in anticipation of the arrival of specialized personnel and trained hostage negotiators. However, it is understood that hostage situations are dynamic and can require that officers react quickly to developing or changing threats. The following options while not all-inclusive or in any particular order, should be considered:

- (a) Ensure injured persons are evacuated from the immediate threat area if it is reasonably safe to do so. Request medical assistance.
- (b) Assign personnel to a contact team to control the subject should he/she attempt to exit the building, structure or vehicle, and attack, use deadly force, attempt to escape or surrender prior to additional resources arriving.
- (c) Establish a rapid response team in the event it becomes necessary to rapidly enter a building, structure or vehicle, such as when the suspect is using deadly force against any hostages (see the Rapid Response and Deployment Policy).
- (d) Assist hostages or potential hostages to escape if it is reasonably safe to do so. Hostages should be kept separated if practicable pending further interview.
- (e) Request additional personnel, resources and equipment as needed (e.g., canine team, air support).
- (f) Provide responding emergency personnel with a safe arrival route to the location.
- (g) Evacuate non-injured persons in the immediate threat area if it is reasonably safe to do so.
- (h) Coordinate pursuit or surveillance vehicles and control of travel routes.
- (i) Attempt or obtain a line of communication and gather as much information about the suspect as possible, including any weapons, victims and their injuries, additional hazards, other involved parties and any other relevant intelligence information.
- (j) Establish an inner and outer perimeter as resources and circumstances permit to prevent unauthorized access.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Hostage and Barricade Incidents

- (k) Evacuate bystanders, residents and businesses within the inner and then outer perimeter as appropriate. Check for injuries, the presence of other involved subjects, witnesses, evidence or additional information.
- (l) Determine the need for and notify the appropriate persons within and outside the Department, such as command officers and the Public Information Officer.
- (m) If necessary and available, establish a tactical or exclusive radio frequency for the incident.

407.5 SUPERVISOR RESPONSIBILITIES

Upon being notified that a hostage or barricade situation exists, the supervisor should immediately respond to the scene, assess the risk level of the situation, establish a proper chain of command and assume the role of Incident Commander until properly relieved. This includes requesting a Special Weapons and Tactics Unit (SWAT) response if appropriate and apprising the SWAT Commander of the circumstances. In addition, the following options, listed here in no particular order, should be considered:

- (a) Ensure injured persons are evacuated and treated by medical personnel.
- (b) Ensure the completion of necessary first responder responsibilities or assignments.
- (c) Request crisis negotiators, specialized units, additional personnel, resources or equipment as appropriate.
- (d) Establish a command post location as resources and circumstances permit.
- (e) Designate assistants who can help with intelligence information and documentation of the incident.
- (f) If it is practicable to do so, arrange for video documentation of the operation.
- (g) Consider contacting utility and communication providers when restricting such services (e.g., restricting electric power, gas, telephone service).
- (h) Ensure adequate law enforcement coverage for the remainder of the City during the incident. The supervisor should direct non-essential personnel away from the scene unless they have been summoned by the supervisor or Dispatch.
- (i) Identify a media staging area outside the outer perimeter and have the department Public Information Officer or a designated temporary media representative provide media access in accordance with the News Media Relations Policy.
- (j) Identify the need for mutual aid and the transition or relief of personnel for incidents of extended duration.
- (k) Debrief personnel and review documentation as appropriate.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Hostage and Barricade Incidents

407.6 CRISIS RESPONSE UNIT RESPONSIBILITIES

It will be the Incident Commander's decision, with input from the SWAT Commander, whether to deploy the SWAT during a hostage or barricade situation. Once the Incident Commander authorizes deployment, the SWAT Commander or the authorized designee will be responsible for the tactical portion of the operation. The Incident Commander shall continue supervision of the command post operation, outer perimeter security and evacuation, media access and support for the SWAT. The Incident Commander and the SWAT Commander or the authorized designee shall maintain communications at all times.

407.7 REPORTING

Unless otherwise relieved by a supervisor or Incident Commander, the handling officer at the scene is responsible for completion and/or coordination of incident reports.

Response to Bomb Calls

408.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines to assist members of the South Salt Lake Police Department in their initial response to incidents involving explosives, explosive devices, explosion/ bombing incidents or threats of such incidents. Under no circumstances should these guidelines be interpreted as compromising the safety of first responders or the public. When confronted with an incident involving explosives, safety should always be the primary consideration.

408.1.1 POLICY

- (a) The following procedures shall be used when responding to bomb threats and bomb emergencies:
 - 1. Establish a command post or center.
 - 2. Decide what primary or alternate communications will be used.
 - 3. Establish clearly who will evaluate the bomb threat and how this will be accomplished.
 - (a) If there is a suspicious package the evaluation should be performed by a bomb tech.
 - (b) If there is no known device, the explosives detection handler and the bomb tech(s) should make the decision.
 - 4. Decide what procedures will be followed when a bomb threat is received and/ or a device is discovered.
 - (a) An on-duty Sergeant or Watch Commander shall consider the evacuation of a building or an area if incident is only a threat, with no device located.
 - (b) If a device is located, the on-duty Sergeant or Watch Commander shall judge the size of the device make a determination of the appropriate evacuation distance.
 - 5. Any decisions about handling a bomb incident should take into consideration secondary issues, such as the proximity of a chemical plant, railroad, and/or fuel storage complex.

408.2 POLICY

It is the policy of the South Salt Lake Police Department to place a higher priority on the safety of persons and the public over damage or destruction to public or private property.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Response to Bomb Calls

408.3 RECEIPT OF BOMB THREAT

Department members receiving a bomb threat should obtain as much information from the individual as reasonably possible, including the type, placement and alleged detonation time of the device.

If the bomb threat is received on a recorded line, reasonable steps should be taken to ensure that the recording is preserved in accordance with established department evidence procedures.

The member receiving the bomb threat should ensure that the Watch Commander is immediately advised and informed of the details. This will enable the Watch Commander to ensure that the appropriate personnel are dispatched and, as appropriate, the threatened location is given an advance warning.

408.4 GOVERNMENT FACILITY OR PROPERTY

A bomb threat targeting a government facility may require a different response based on the government agency.

408.4.1 SOUTH SALT LAKE POLICE DEPARTMENT FACILITY

If the bomb threat is against the South Salt Lake Police Department facility, the Watch Commander will direct and assign officers as required for coordinating a general building search or evacuation of the police department, as he/she deems appropriate.

408.4.2 OTHER COUNTY OR MUNICIPAL FACILITY OR PROPERTY

If the bomb threat is against a county or municipal facility within the jurisdiction of the South Salt Lake Police Department that is not the property of this department, the appropriate agency will be promptly informed of the threat. Assistance to the other entity may be provided as the Watch Commander deems appropriate.

408.4.3 FEDERAL BUILDING OR PROPERTY

If the bomb threat is against a federal building or property, the Federal Protective Service should be immediately notified. The Federal Protective Service provides a uniformed law enforcement response for most facilities, which may include use of its Explosive Detector Dog teams.

If the bomb threat is against a federal government property where the Federal Protective Service is unable to provide a timely response, the appropriate facility's security or command staff should be notified.

Bomb threats against a military installation should be reported to the military police or other military security responsible for the installation.

408.5 PRIVATE FACILITY OR PROPERTY

When a member of this department receives notification of a bomb threat at a location in the City of South Salt Lake, the member receiving the notification should obtain as much information as reasonably possible from the notifying individual, including:

- (a) The location of the facility.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Response to Bomb Calls

- (b) The nature of the threat.
- (c) Whether the type and detonation time of the device is known.
- (d) Whether the facility is occupied and, if so, the number of occupants currently on-scene.
- (e) Whether the individual is requesting police assistance at the facility.
- (f) Whether there are any internal facility procedures regarding bomb threats in place, such as:
 - 1. No evacuation of personnel and no search for a device.
 - 2. Search for a device without evacuation of personnel.
 - 3. Evacuation of personnel without a search for a device.
 - 4. Evacuation of personnel and a search for a device.

The member receiving the bomb threat information should ensure that the Watch Commander is immediately notified so that he/she can communicate with the person in charge of the threatened facility.

408.5.1 ASSISTANCE

The Watch Commander should be notified when police assistance is requested. The Watch Commander will make the decision whether the Department will render assistance and at what level. Information and circumstances that indicate a reasonably apparent, imminent threat to the safety of either the facility or the public may require a more active approach, including police control over the facility.

Should the Watch Commander determine that the Department will assist or control such an incident, he/she will determine:

- (a) The appropriate level of assistance.
- (b) The plan for assistance.
- (c) Whether to evacuate and/or search the facility.
- (d) Whether to involve facility staff in the search or evacuation of the building.
 - 1. The person in charge of the facility should be made aware of the possibility of damage to the facility as a result of a search.
 - 2. The safety of all participants is the paramount concern.
- (e) The need for additional resources, including:
 - 1. Notification and response, or standby notice, for fire and emergency medical services.

Even though a facility does not request police assistance to clear the interior of a building, based upon the circumstances and known threat, officers may be sent to the scene to evacuate other areas that could be affected by the type of threat, or for traffic and pedestrian control.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Response to Bomb Calls

408.6 FOUND DEVICE

When handling an incident involving a suspected explosive device, the following guidelines, while not all inclusive, should be followed:

- (a) No known or suspected explosive item should be considered safe regardless of its size or apparent packaging.
- (b) The device should not be touched or moved except by the bomb squad or military explosive ordnance disposal team.
- (c) Personnel should not transmit on any equipment that is capable of producing radio frequency energy within the evacuation area around the suspected device. This includes the following:
 - 1. Two-way radios
 - 2. Cell phones
 - 3. Other personal communication devices
- (d) The appropriate bomb squad or military explosive ordnance disposal team should be summoned for assistance.
- (e) The largest perimeter reasonably possible should initially be established around the device based upon available personnel and the anticipated danger zone.
- (f) A safe access route should be provided for support personnel and equipment.
- (g) Search the area for secondary devices as appropriate and based upon available resources.
- (h) Consider evacuation of buildings and personnel near the device or inside the danger zone and the safest exit route.
- (i) Promptly relay available information to the Watch Commander including:
 - 1. The time of discovery.
 - 2. The exact location of the device.
 - 3. A full description of the device (e.g., size, shape, markings, construction).
 - 4. The anticipated danger zone and perimeter.
 - 5. The areas to be evacuated or cleared.

408.7 EXPLOSION/BOMBING INCIDENTS

When an explosion has occurred, there are multitudes of considerations which may confront the responding officers. As in other catastrophic events, a rapid response may help to minimize injury to victims, minimize contamination of the scene by gathering crowds, or minimize any additional damage from fires or unstable structures.

408.7.1 CONSIDERATIONS

Officers responding to explosions, whether accidental or a criminal act, should consider the following actions:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Response to Bomb Calls

- (a) Assess the scope of the incident, including the number of victims and extent of injuries.
- (b) Request additional personnel and resources, as appropriate.
- (c) Assist with first aid.
- (d) Identify and take appropriate precautions to mitigate scene hazards, such as collapsed structures, bloodborne pathogens and hazardous materials.
- (e) Assist with the safe evacuation of victims, if possible.
- (f) Establish an inner perimeter to include entry points and evacuation routes. Search for additional or secondary devices.
- (g) Preserve evidence.
- (h) Establish an outer perimeter and evacuate if necessary.
- (i) Identify witnesses.

408.7.2 NOTIFICATIONS

When an explosion has occurred, the following people should be notified as appropriate:

- Fire department
- Bomb squad
- Additional department personnel, such as investigators and forensic services
- Field supervisor
- Watch Commander
- Other law enforcement agencies, including local, state or federal agencies, such as the FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
- Other government agencies, as appropriate

408.7.3 CROWD CONTROL

Only authorized members with a legitimate need should be permitted access to the scene. Spectators and other unauthorized individuals should be restricted to a safe distance as is reasonably practicable given the available resources and personnel.

408.7.4 PRESERVATION OF EVIDENCE

As in any other crime scene, steps should immediately be taken to preserve the scene. The Watch Commander should assign officers to protect the crime scene area, which could extend over a long distance. Consideration should be given to the fact that evidence may be imbedded in nearby structures or hanging in trees and bushes.

Involuntary Commitments

409.1 PURPOSE AND SCOPE

This policy provides guidelines for when officers may place an individual under involuntary commitment.

409.2 POLICY

It is the policy of the South Salt Lake Police Department to protect the public and individuals through legal and appropriate use of the involuntary commitment process.

409.3 AUTHORITY

An officer may take a person into protective custody to be temporarily involuntarily committed to a local mental health authority when that officer has probable cause, based on their observation of the individual, to believe (Utah Code 26B-5-331; Utah Code 26B-5-403):

- (a) The person has a mental illness.
- (b) The person poses a substantial danger to themselves or others because of their mental illness and conduct.
- (c) If the person is a child, they will benefit from mental health care and treatment and there is no appropriate less-restrictive alternative.

409.3.1 VOLUNTARY EVALUATION

If an officer encounters an individual who may qualify for an involuntary commitment, the officer may inquire as to whether the person desires to voluntarily be evaluated at an appropriate facility. If the person so desires, the officers should:

- (a) Transport the person to an appropriate facility that is able to conduct the evaluation and admit the person.
- (b) Document the circumstances surrounding the individual's desire to pursue voluntary evaluation and/or admission.

If at any point the person changes their mind regarding voluntary evaluation, officers should proceed with the involuntary commitment, if appropriate.

409.3.2 RESTRAINTS

If the patient is violent or potentially violent, the officer will notify the staff of this concern. The staff member in charge will have discretion as to whether soft-restraints will be used. If these restraints are desired, the officer will wait while they are being applied to help provide physical control of the patient, if needed.

409.3.3 MENTAL HEALTH DOCUMENTATION

The officer will complete the prescribed form and provide it to the staff member assigned to that patient. The officer will retain a copy of the 24-hour evaluation for inclusion in the case report. The officer shall also provide a verbal summary to an emergency department staff member regarding the circumstances leading to the involuntary commitment.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Involuntary Commitments

409.3.4 SECURING OF WEAPONS

If a receiving and secured facility prohibits weapons or if an extraordinary event occurs in the treatment facility and officers determine a need to secure their firearms, the firearm shall be secured in the appropriate gun locker at the facility or in the police vehicle.

409.4 TRANSPORTATION

A person taken into custody for a civil commitment should be transported to a facility designated by the local mental health authority as follows (Utah Code 26B-5-331):

- (a) The person should be transported by ambulance if they meet any of the criteria described in Utah Code 53-2d-405 or transportation arrangements have been made by a physician, designated examiner, or mental health officer and the officer's presence is not necessary for public safety.
 - 1. If the person requires physical medical attention, they should be transported by ambulance to an appropriate medical facility.
- (b) When the person is not transported by ambulance and the designated facility is within the jurisdiction of the South Salt Lake Police Department, the person should be transported by the detaining officer in accordance with the Transporting Persons in Custody Policy.
 - 1. If the designated facility is outside of this [city/county]'s jurisdiction, a request should be made to the appropriate agency to transport the person to the designated facility.

409.5 TRANSFER TO APPROPRIATE FACILITY

Upon arrival at the facility, the officer will escort the individual into a treatment area designated by a facility staff member. If the individual is not seeking treatment voluntarily, the officer should provide the staff member with the written application for an involuntary commitment and remain present to provide clarification of the grounds for detention, upon request.

Absent exigent circumstances, the transporting officer should not assist facility staff with the admission process, including restraint of the individual. However, if the individual is transported and delivered while restrained, the officer may assist with transferring the individual to facility restraints and will be available to assist during the admission process, if requested. Under normal circumstances, officers will not apply facility-ordered restraints.

409.6 DOCUMENTATION

The officer shall complete an application for commitment, using the form prescribed by the Division of Substance Abuse and Mental Health, provide it to the facility staff member assigned to the individual, and retain a copy of the application for inclusion in the case report (Utah Code 26B-5-331).

The officer should also provide a verbal summary to any evaluating staff member regarding the circumstances leading to the involuntary detention.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Involuntary Commitments

409.7 CRIMINAL OFFENSES

Officers investigating an individual who is suspected of committing a minor criminal offense and who is being taken into custody through an involuntary commitment should resolve the criminal matter by issuing a warning or a citation, as appropriate.

When an individual who may qualify for an involuntary commitment has committed a serious criminal offense that would normally result in an arrest and transfer to a jail facility, the officer should:

- (a) Arrest the individual when there is probable cause to do so.
- (b) Notify the appropriate supervisor of the facts supporting the arrest and the facts that would support the detention.
- (c) Facilitate the individual's transfer to the jail facility.
- (d) Thoroughly document in the related reports the circumstances that indicate the individual may qualify for an involuntary commitment.

In the supervisor's judgment, the individual may instead be transported to the appropriate mental health facility. The supervisor should consider the seriousness of the offense, the treatment options available, the ability of this [department/office] to regain custody of the individual, [department/office] resources (e.g., posting a guard), and other relevant factors in making this decision.

409.8 FIREARMS AND OTHER WEAPONS

Whenever a person is taken into custody for a civil commitment, the handling officers should seek to determine if the person owns or has access to any firearm or other deadly weapon. Officers should consider whether it is appropriate and consistent with current search and seizure law under the circumstances to seize any such firearms or other dangerous weapons (e.g. safekeeping, evidence, consent).

Officers are cautioned that a search warrant may be needed before entering a residence or other place to search, unless lawful warrantless entry has already been made (e.g., exigent circumstances, consent). A warrant may also be needed before searching for or seizing weapons.

The handling officer should further advise the person of the procedure for the return of any firearm or other weapon that has been taken into custody.

409.9 TRAINING

This [department/office] will endeavor to provide POST-approved training on interaction with persons with a mental disability, involuntary commitments, and crisis intervention.

Citation Releases

410.1 PURPOSE AND SCOPE

The purpose of this policy is to provide members of the South Salt Lake Police Department with guidance on when to release adults who are suspected offenders on a citation for a criminal offense, rather than having the person held in custody for a court appearance or released on bail.

Additional release restrictions may apply to those detained for domestic violence, as outlined in the Domestic Violence Policy.

410.2 POLICY

The South Salt Lake Police Department will consider its resources and its mission of protecting the community when exercising any discretion to release suspected offenders on a citation, when authorized to do so.

410.3 RELEASE

A suspected offender may be released on issuance of a citation as follows:

- (a) When the person is arrested for a misdemeanor or infraction charge (Utah Code 77-7-18).
- (b) When a warrant has been issued by a magistrate who has included in the order that the person be released on a summons (U. R. Crim. P. Rule 6).

410.4 PROHIBITIONS

The release of a suspected offender on a citation is not permitted if prohibited by local court rule.

See the Domestic Violence Policy for release restrictions related to those investigations.

410.5 CONSIDERATIONS

In determining whether to cite and release a person when discretion is permitted, officers should consider:

- (a) The type of offense committed.
- (b) The known criminal history of the suspected offender.
- (c) The ability to identify the suspected offender with reasonable certainty.
- (d) Whether there is any record of the individual failing to appear in previous cases or other articulable indications that the individual may not appear in court for this offense.
- (e) The individual's ties to the area, such as residence, employment or family.
- (f) Whether there is reasonable likelihood that criminal conduct by the individual will continue.

410.6 STATE PRIVILEGES

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Citation Releases

410.6.1 LEGISLATIVE PRIVILEGE

Members of the Legislature shall not be subject to civil arrest during each general and special session of the Legislature or for 15 days immediately preceding and following each session, except for any felony, treason, or breach of the peace. Legislators may be issued a citation and a summons to appear at a date outside of the time of legislative privilege (Utah Constitution Article VI § 8).

410.6.2 VOTER PRIVILEGE

A person who attends an election or who is traveling to and from a voting location shall not be subject to civil arrest on an election day, except for an act of treason, a felony, or a breach of the peace (Utah Constitution Article IV § 3).

Rapid Response and Deployment

411.1 PURPOSE AND SCOPE

Violence that is committed in schools, workplaces and other locations by individuals or a group of individuals who are determined to target and kill persons and to create mass casualties presents a difficult situation for law enforcement. The purpose of this policy is to identify guidelines and factors that will assist responding officers in situations that call for rapid response and deployment.

411.2 POLICY

The South Salt Lake Police Department will endeavor to plan for rapid response to crisis situations, and to coordinate response planning with other emergency services as well as with those that are responsible for operating sites that may be the target of a critical incident.

Nothing in this policy shall preclude the use of reasonable force, deadly or otherwise, by members of the Department in protecting themselves or others from death or serious injury.

411.3 FIRST RESPONSE

If there is a reasonable belief that acts or threats by a suspect are placing lives in imminent danger, first responding officers should consider reasonable options to reduce, prevent or eliminate the threat. Officers must decide, often under a multitude of difficult and rapidly evolving circumstances, whether to advance on the suspect, take other actions to deal with the threat or wait for additional resources.

If a suspect is actively engaged in the infliction of serious bodily harm or other life-threatening activity toward others, officers should take immediate action, if reasonably practicable, while requesting additional assistance.

Officers should remain aware of the possibility that an incident may be part of a coordinated multi-location attack that may require some capacity to respond to other incidents at other locations.

When deciding on a course of action officers should consider:

- (a) Whether to advance on or engage a suspect who is still a possible or perceived threat to others. Any advance or engagement should be based on information known or received at the time.
- (b) Whether to wait for additional resources or personnel. This does not preclude an individual officer from taking immediate action.
- (c) Whether individuals who are under imminent threat can be moved out of danger or evacuated with reasonable safety.
- (d) Whether the suspect can be contained or denied access to victims.
- (e) Whether the officers have the ability to effectively communicate with other personnel or resources.
- (f) Whether planned tactics can be effectively deployed.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Rapid Response and Deployment

- (g) The availability of rifles, shotguns, shields, breaching tools, control devices and any other appropriate tools, and whether the deployment of these tools will provide a tactical advantage.

In a case of a barricaded suspect with no hostages and no immediate threat to others, officers should consider summoning and waiting for additional assistance (special tactics and/or hostage negotiation team response).

411.4 CONSIDERATIONS

When dealing with a crisis situation members should:

- (a) Assess the immediate situation and take reasonable steps to maintain operative control of the incident.
- (b) Obtain, explore and analyze sources of intelligence and known information regarding the circumstances, location and suspect involved in the incident.
- (c) Attempt to attain a tactical advantage over the suspect by reducing, preventing or eliminating any known or perceived threat.
- (d) Attempt, if feasible and based upon the suspect's actions and danger to others, a negotiated surrender of the suspect and release of the hostages.

411.5 PLANNING

The Administrative Lieutenant should coordinate critical incident planning. Planning efforts should consider:

- (a) Identification of likely critical incident target sites, such as schools, shopping centers, entertainment and sporting event venues.
- (b) Availability of building plans and venue schematics of likely critical incident target sites.
- (c) Communications interoperability with other law enforcement and emergency service agencies.
- (d) Training opportunities in critical incident target sites, including joint training with site occupants.
- (e) Evacuation routes in critical incident target sites.
- (f) Patrol first-response training.
- (g) Response coordination and resources of emergency medical and fire services.
- (h) Equipment needs.
- (i) Mutual aid agreements with other agencies.
- (j) Coordination with private security providers in critical incident target sites.

411.6 TRAINING

The Training Coordinator should include rapid response to critical incidents in the training plan. This training should address:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Rapid Response and Deployment

- (a) Orientation to likely critical incident target sites, such as schools, shopping centers, entertainment and sporting event venues.
- (b) Communications interoperability with other law enforcement and emergency service agencies.
- (c) Patrol first-response training, including patrol rifle, shotgun, breaching tool and control device training.
- (d) First aid, including gunshot trauma.
- (e) Reality-based scenario training (e.g., active shooter, disgruntled violent worker).

Police Escorts

412.1 PURPOSE

The purpose of this policy is to outline specific circumstances under which police escorts may be provided and to identify departmental personnel authorized to approve the request for an escort.

412.2 POLICY

The South Salt Lake Police Department will provide vehicular police escort services to the community on a limited approved basis. Escort services will only be approved if they can be provided in a manner that will ensure the safety of the public, officers and allow for orderly and expeditious flow of traffic.

412.3 FUNERAL ESCORTS

Requests for funeral escorts will be the primary responsibility of the patrol division. All request for a funeral escort shall be approved through the Chief's office. Approval should be based on the totality of the circumstances with consideration for the following:

Type of area

Time of Day

Traffic Volume

Available Staffing

Any unique or specific circumstances that could potentially affect the safety or orderly movement of the procession and escort.

412.4 FUNERAL ESCORT PROCEDURES

All officers escorting a funeral procession will use their emergency lights to increase visibility throughout the escort.

While conducting a funeral escort, officers should comply with the applicable state statutes and City ordinances related to traffic signals and funeral escorts,

Whenever practicable and appropriate, intersections along the funeral procession route should be closed/blocked to cross traffic during the escort.

412.5 DIGNITARY ESCORTS

Request for dignitary escorts by other governmental agencies will be forwarded to the Chief's office. (either the Chief of Police or Deputy Chief) Dignitary protection details are high-stakes operations designed to ensure the safety and security of high profile individuals such as governmental officials, diplomats, corporate executives, and other significant personnel.

Prior to providing assistance there should a planning and risk assessment, threat assessment, intelligence gathering of possible threats, route and location analysis, communication and established channels between teams. Movement and transportation procedures should be

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Police Escorts

clarified between both team as to a convoy formation, decoy vehicles, route monitoring and an immediate response action plan.

The South Salt Lake Police Department will provide assistance after an operation plan has been agreed upon by both agencies.

Dignitary Protective details could involve the movement of a person who has a protective detail.

412.6 HAZARD ESCORTS

A hazard escort may involve oversize vehicles and/or vehicles transporting hazardous materials. Officers conducting a hazard escort will be expected to comply with all regulations and should follow an operational plan developed during the approval process. Intersections along the route of the a hazard escort may be staffed by police personnel and closed/blocked to cross traffic during the escort, if appropriate.

412.7 CIVIC EVENTS

Examples of this type of escort include, but are not limited to, parades, marches, the return of military service members from deployments, and honoring local sports teams or organizations.

412.8 MEDICAL EMERGENCY ESCORTS

Officers should not provide emergency escorts to another emergency vehicle which has its own emergency signaling devices except in the following situations:

The emergency equipment on an emergency vehicle is malfunctioning;

The driver of an emergency vehicle is not familiar with the area and requests assistance to the destination;

When authorized by a supervisor.

Officers will not provide emergency escorts to civilian vehicles. If a medical emergency exists, the officer will request the assistance of emergency medical services to transport the subject with the medical need.

Any person following the patient or victim to the appropriate medical facility should be directed to proceed at normal speed and in compliance with all traffic regulations.

Immigration Violations

413.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines to members of the South Salt Lake Police Department relating to immigration and interacting with federal immigration officials

413.2 POLICY

It is the policy of the South Salt Lake Police Department that all members make personal and professional commitments to equal enforcement of the law and equal service to the public. Confidence in this commitment will increase the effectiveness of this [department/office] in protecting and serving the entire community and recognizing the dignity of all persons, regardless of their national origin or immigration status.

In keeping with this commitment, race, color, or national origin will not be considered under this policy except to the extent permitted by the constitutions of the United States and Utah (Utah Code § 76-14-202).

413.3 VICTIMS AND WITNESSES

To encourage crime reporting and cooperation in the investigation of criminal activity, all individuals, regardless of their immigration status, must feel secure that contacting or being addressed by members of law enforcement will not automatically lead to immigration inquiry and/or deportation. While it may be necessary to determine the identity of a victim or witness, members shall treat all individuals equally and not in any way that would violate the United States or Utah constitutions.

413.4 DETENTIONS

An officer should not detain any individual, for any length of time, for a civil violation of federal immigration laws or a related civil warrant.

An officer who has a reasonable suspicion that an individual already lawfully contacted or detained has committed a criminal violation of federal immigration law may detain the person for a reasonable period of time in order to contact federal immigration officials to verify whether an immigration violation is a federal civil violation or a criminal violation. If the violation is a criminal violation, the officer may continue to detain the person for a reasonable period of time if requested by federal immigration officials (8 USC § 1357(g)(10)). No individual who is otherwise ready to be released should continue to be detained only because questions about the individual's status are unresolved.

If the officer has facts that establish probable cause to believe that a person already lawfully detained has committed a criminal immigration offense, he/she may continue the detention and may request a federal immigration official to respond to the location to take custody of the detained person (8 USC § 1357(g)(10)).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Immigration Violations

An officer is encouraged to forgo detentions made solely on the basis of a misdemeanor offense when time limitations, availability of personnel, issues of officer safety, communication capabilities, or the potential to obstruct a separate investigation outweigh the need for the detention.

An officer should notify a supervisor as soon as practicable whenever an individual is being detained for a criminal immigration violation.

413.4.1 INVESTIGATING HUMAN TRAFFICKING OR SMUGGLING

When an officer conducts a lawful traffic stop and reasonably suspects that any person in the vehicle is violating Utah human trafficking or human smuggling laws, the officer shall investigate the suspected violations and inquire into the immigration status of the occupants of the vehicle. An officer may not delay or postpone addressing the original purpose of the stop merely to confirm a person's immigration status (Utah Code 76-14-202).

413.4.2 VERIFICATION OF IMMIGRATION STATUS

A person's citizenship or immigration status shall be verified whenever the person is lawfully arrested for a felony or misdemeanor offense and is unable to provide an identifying document as listed in Utah Code 76-14-203 and the officer is otherwise unable to verify the identity of the person. Verification of immigration status should take place at the time of the booking and not in the field (Utah Code 76-14-202).

413.4.3 SUPERVISOR RESPONSIBILITIES

When notified that an officer has detained an individual and established reasonable suspicion or probable cause to believe the person has violated a criminal immigration offense, the supervisor should determine whether it is appropriate to:

- (a) Transfer the person to federal authorities.
- (b) Lawfully arrest the person for a criminal offense or pursuant to a judicial warrant (see the Law Enforcement Authority Policy).

413.5 ARREST NOTIFICATION TO FEDERAL IMMIGRATION OFFICIALS

Generally, an officer should not notify federal immigration officials when booking arrestees at a jail facility. Any required notification will be handled according to jail operation procedures. No individual who is otherwise ready to be released should continue to be detained solely for the purpose of notification.

413.6 FEDERAL REQUESTS FOR ASSISTANCE

Requests by federal immigration officials for assistance from this [department/office] should be directed to a supervisor. The [Department/Office] may provide available support services, such as traffic control or peacekeeping efforts.

413.7 INFORMATION SHARING

No member of this [department/office] will prohibit, or in any way restrict, any other member from doing any of the following regarding the citizenship or immigration status, lawful or unlawful, of any individual (8 USC § 1373):

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Immigration Violations

- (a) Sending information to, or requesting or receiving such information from federal immigration officials
- (b) Maintaining such information in [department/office] records
- (c) Exchanging such information with any other federal, state, or local government entity

413.7.1 IMMIGRATION DETAINERS

No individual should be held based solely on a federal immigration detainer under 8 CFR 287.7 unless the person has been charged with a federal crime or the detainer is accompanied by a warrant, affidavit of probable cause, or removal order. Notification to the federal authority issuing the detainer should be made prior to the release.

413.8 U VISA AND T VISA NONIMMIGRANT STATUS

Under certain circumstances, federal law allows temporary immigration benefits, known as a U visa, to victims and witnesses of certain qualifying crimes (8 USC § 1101(a)(15)(U)).

Similar immigration protection, known as a T visa, is available for certain qualifying victims of human trafficking (8 USC § 1101(a)(15)(T)).

Any request for assistance in applying for U visa or T visa status should be forwarded in a timely manner to the Victim Advocate Supervisor, who will coordinate with Special Victim's Unit Detective Sergeant.

Investigations Division supervisor assigned to oversee the handling of any related case. The Investigations Division supervisor should:

- (a) Consult with the assigned investigator to determine the current status of any related case and whether further documentation is warranted.
- (b) Contact the appropriate prosecutor assigned to the case, if applicable, to ensure the certification or declaration has not already been completed and whether a certification or declaration is warranted.
- (c) Address the request and complete the certification or declaration, if appropriate, in a timely manner.
 - 1. The instructions for completing certification and declaration forms can be found on the U.S. Department of Homeland Security (DHS) website.
- (d) Ensure that any decision to complete, or not complete, a certification or declaration form is documented in the case file and forwarded to the appropriate prosecutor. Include a copy of any completed form in the case file.

Once task a-c have been completed, the packet of information should be reviewed and submitted to the Chief's office for final approval.

413.8.1 U NONIMMIGRANT STATUS GUIDELINES

U nonimmigrant status requests shall be processed and maintained in a manner consistent with Utah Code 77-38-503 and federal guidelines.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Immigration Violations

The Investigation Division Commander should ensure certification requests conducted by this agency are processed within 90 days of request, unless the noncitizen is in removal proceedings, in which case the certification should be processed within 14 days of request (Utah Code 77-38-503).

413.8.2 REPORTING REQUIREMENTS

Before June 30 of each year, the Chief of Police or designee shall submit a report of the following information to the Commission on Criminal and Juvenile Justice (Utah Code 77-38-503):

- (a) The number of victims that requested U nonimmigrant certifications from the agency
- (b) The number of U nonimmigrant certifications that were signed
- (c) The number of U nonimmigrant certifications that were denied

413.9 TRAINING

The Training Coordinator should ensure that officers receive training on this policy.

Training should include:

- (a) Identifying civil versus criminal immigration violations.
- (b) Factors that may be considered in determining whether a criminal immigration offense has been committed.

Emergency Utility Service

414.1 PURPOSE AND SCOPE

The City public works department has personnel available to handle emergency calls 24 hours per day. Calls for service during non-business hours are frequently directed to the Department. Requests for such service received by this department should be handled in the following manner.

414.1.1 BROKEN WATER LINES

The City's responsibility ends at the water meter; any break or malfunction in the water system from the water meter to the citizen's residence or business is the customer's responsibility. Public works can only turn off the valve at the meter. The citizen can normally accomplish this.

If a break occurs on the City side of the meter, emergency personnel should be called as soon as practical by Dispatch.

414.1.2 ELECTRICAL LINES

City Public Works does not maintain electrical lines to street light poles. When a power line poses a hazard, an officer should be dispatched to protect against personal injury or property damage that might be caused by power lines. The electric company or public works should be promptly notified, as appropriate.

414.1.3 EMERGENCY NUMBERS

A current list of emergency personnel who are to be called for municipal utility emergencies is maintained by Dispatch.

Aircraft Accidents

415.1 PURPOSE AND SCOPE

The purpose of this policy is to provide department members with guidelines for handling aircraft accidents.

This policy does not supersede, and is supplementary to, applicable portions of the Crime and Disaster Scene Integrity, Emergency Management Plan and Hazardous Material Response policies.

415.1.1 DEFINITIONS

Definitions related to this policy include:

Aircraft - Any fixed wing aircraft, rotorcraft, balloon, blimp/dirigible or glider that is capable of carrying a person or any unmanned aerial vehicle other than those intended for non-commercial recreational use.

415.2 POLICY

It is the policy of the South Salt Lake Police Department to provide an appropriate emergency response to aircraft accidents. This includes emergency medical care and scene management.

415.3 ARRIVAL AT SCENE

Officers or other authorized members tasked with initial scene management should establish an inner and outer perimeter to:

- (a) Protect persons and property.
- (b) Prevent any disturbance or further damage to the wreckage or debris, except to preserve life or rescue the injured.
- (c) Preserve ground scars and marks made by the aircraft.
- (d) Manage the admission and access of public safety and medical personnel to the extent necessary to preserve life or to stabilize hazardous materials.
- (e) Maintain a record of persons who enter the accident site.
- (f) Consider implementation of an Incident Command System (ICS).

415.4 INJURIES AND CASUALTIES

Members should address emergency medical issues and provide care as a first priority.

Those tasked with the supervision of the scene should coordinate with the National Transportation Safety Board (NTSB) before the removal of bodies. If that is not possible, the scene supervisor should ensure documentation of what was disturbed, including switch/control positions and instrument/gauge readings.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Aircraft Accidents

415.5 NOTIFICATIONS

When an aircraft accident is reported to this department, the responding supervisor shall ensure notification is or has been made to NTSB, the Federal Aviation Administration (FAA), and when applicable, the appropriate branch of the military.

Supervisors shall ensure other notifications are made once an aircraft accident has been reported. The notifications will vary depending on the type of accident, extent of injuries or damage, and the type of aircraft involved. When an aircraft accident has occurred, it is generally necessary to notify the following:

- (a) Fire department
- (b) Appropriate airport tower
- (c) Emergency medical services (EMS)

415.6 CONTROLLING ACCESS AND SCENE AUTHORITY

Prior to NTSB arrival, scene access should be limited to authorized personnel from the:

- (a) FAA.
- (b) Fire department, EMS or other assisting law enforcement agencies.
- (c) Medical Examiner.
- (d) Air Carrier/Operators investigative teams with NTSB approval.
- (e) Appropriate branch of the military, when applicable.
- (f) Other emergency services agencies (e.g., hazardous materials teams, biohazard decontamination teams, fuel recovery specialists, explosive ordnance disposal specialists).

The NTSB has primary responsibility for investigating accidents involving civil aircraft. In the case of a military aircraft accident, the appropriate branch of the military will have primary investigation responsibility.

After the NTSB or military representative arrives on-scene, the efforts of this department will shift to a support role for those agencies.

If NTSB or a military representative determines that an aircraft or accident does not qualify under its jurisdiction, the on-scene department supervisor should ensure the accident is still appropriately investigated and documented.

415.7 DANGEROUS MATERIALS

Members should be aware of potentially dangerous materials that might be present. These may include, but are not limited to:

- (a) Fuel, chemicals, explosives, biological or radioactive materials and bombs or other ordnance.
- (b) Pressure vessels, compressed gas bottles, accumulators and tires.
- (c) Fluids, batteries, flares and igniters.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Aircraft Accidents

- (d) Evacuation chutes, ballistic parachute systems and composite materials.

415.8 DOCUMENTATION

All aircraft accidents occurring within the City of South Salt Lake shall be documented. At a minimum the documentation should include the date, time and location of the incident; any witness statements, if taken; the names of SSLPD members deployed to assist; other City resources that were utilized; and cross reference information to other investigating agencies. Suspected criminal activity should be documented on the appropriate crime report.

415.8.1 WRECKAGE

When reasonably safe, members should:

- (a) Obtain the aircraft registration number (N number) and note the type of aircraft.
- (b) Attempt to ascertain the number of casualties.
- (c) Obtain photographs or video of the overall wreckage, including the cockpit and damage, starting at the initial point of impact, if possible, and any ground scars or marks made by the aircraft.
 - 1. Military aircraft may contain classified equipment and therefore shall not be photographed unless authorized by a military commanding officer (18 USC § 795).
- (d) Secure, if requested by the lead authority, any electronic data or video recorders from the aircraft that became dislodged or cell phones or other recording devices that are part of the wreckage.
- (e) Acquire copies of any recordings from security cameras that may have captured the incident.

415.8.2 WITNESSES

Members tasked with contacting witnesses should obtain:

- (a) The location of the witness at the time of his/her observation relative to the accident site.
- (b) A detailed description of what was observed or heard.
- (c) Any photographs or recordings of the accident witnesses may be willing to voluntarily surrender.
- (d) The names of all persons reporting the accident, even if not yet interviewed.
- (e) Any audio recordings of reports to 9-1-1 regarding the accident and dispatch records.

415.9 MEDIA RELATIONS

The Public Information Officer (PIO) should coordinate a response to the media, including access issues, road closures, detours and any safety information that is pertinent to the surrounding community. Any release of information regarding details of the accident itself should be coordinated with the NTSB or other authority who may have assumed responsibility for the investigation.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Aircraft Accidents

Depending on the type of aircraft, the airline or the military may be responsible for family notifications and the release of victims' names. The PIO should coordinate with other involved entities before the release of information.

Field Training Officer Program

416.1 PURPOSE AND SCOPE

The Field Training Program is intended to provide a standardized program to facilitate the officer's transition from the academic setting to the actual performance of general law enforcement duties of the South Salt Lake Police Department.

It is the policy of the Department to assign all new police officers to a structured Field Training Program that is designed to prepare the new officer to perform in a patrol assignment, and possessing all skills needed to operate in a safe, productive and professional manner.

416.1.1 FIELD TRAINING OFFICER DEFINITION

A Field Training Officer (FTO) is an experienced professional who is responsible for training, supervising, and evaluating new employees while they in a real-world setting. An FTO works directly with the trainees during their initial phase of on-the-job training period. They teach practical skills, procedures, and professional standards. They observe performance, give feedback, and document progress. They ensure trainees follow policies, law and safety protocols. They help new employees transition from learning to independent duty responsibilities. An FTO acts as a mentor, evaluator and role model, making sure new personnel are competent, safe, and professional before working on their own.

416.2 FIELD TRAINING OFFICER SELECTION AND TRAINING

The Field Training Officer (FTO) is an experienced officer trained in the art of supervising, training and evaluating entry level and lateral officers in the application of their previously acquired knowledge and skills.

416.2.1 SELECTION PROCESS

FTO's will be selected based on the following requirements:

- (a) Desire to be an FTO.
- (b) Demonstrated ability as a positive role model.
- (c) Evaluation by supervisors and current FTOs.
- (d) Off of probationary status.
- (e) Must not be part of a work improvement plan.

416.2.2 TRAINING

An officer selected as a Field Training Officer shall successfully complete a POST-certified 24-hour Field Training Officer's Course prior to being assigned as an FTO.

416.2.3 FIELD TRAINING OFFICER (FTO) STANDING AND ELIGIBILITY

The Field Training Officer (FTO) role is a position of trust, leadership, and professional influence. To ensure the highest standards of training and mentorship, all FTO's are expected to remain in good standing at all times. Good standing includes consistent adherence to agency policies

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Field Training Officer Program

and procedures, demonstrated professional, satisfactory performance, and conduct that reflects positively on the organization. An FTO who is not in good standing may be temporarily or permanently removed from FTO duties. Such action is not disciplinary in nature, but rather an administrative decision made in the best interest of the trainees, the training program, and the organization. Removal from FTO responsibilities does not preclude future consideration for the role once good standing is restored. This is intended to support the high-quality training environment, promote accountability, and ensure the Field Training Officers continue to serve as effective role models, and mentors.

416.3 FIELD TRAINING OFFICER PROGRAM SUPERVISOR

The Field Training Officer Program is administered by the training sergeant.

The responsibilities of the FTO Program Supervisor include the following:

- (a) Assignment of trainees to FTOs.
- (b) Conduct FTO meetings.
- (c) Maintain and ensure FTO/Trainee performance evaluations are completed.
- (d) Maintain, update and issue the Field Training Manual to each trainee.
- (e) Monitor individual FTO performance.
- (f) Monitor overall FTO Program.
- (g) Maintain liaison with FTO Coordinators of other agencies.
- (h) Maintain liaison with academy staff on recruit performance during the academy.
- (i) Develop ongoing training for FTOs.
- (j) Present recommendation for OIT's early release, release or extension of the FTO training program, to the Chief's office.

416.4 TRAINEE DEFINED

Any entry level or lateral officer newly appointed to the South Salt Lake Police Department who has successfully completed a POST-approved Basic Academy.

416.5 REQUIRED TRAINING

Entry level officers shall be required to successfully complete the 10 week Field Training Program.

The training period for lateral officers may be modified depending on the trainee's demonstrated performance and level of experience.

To the extent practical, entry level and lateral officers should be assigned to a variety of Field Training Officers, shifts and geographical areas during their Field Training Program.

416.6 EVALUATIONS

Evaluations are an important component of the training process and shall be completed as outlined below.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Field Training Officer Program

416.6.1 FIELD TRAINING OFFICER

The FTO will be responsible for the following:

- (a) Complete and submit a written evaluation on the performance of his/her assigned trainee to the FTO program supervisor on a daily basis.
- (b) Review the Daily Trainee Performance Evaluations with the trainee each day.
- (c) Complete a detailed end-of-phase performance evaluation on assigned trainee at the end of each phase of training.
- (d) Sign off all completed topics contained in the Field Training Manual, noting the method(s) of learning and evaluating the performance of his/her assigned trainee.
- (e) Ensure time cards are filled out correctly for all OIT
- (f) FTO's are compensated for providing comprehensive training at the rate of \$70.00 per each shift worked.
- (g) Ensure both City and PD Lexipol policies are reviewed and acknowledge prior to release from the FTO training program.
- (h) The FTO is expected to be the example

416.6.2 IMMEDIATE SUPERVISOR

The immediate supervisor shall review and approve the Daily Trainee Performance Evaluations and forward them to the Field Training Administrator.

416.6.3 FIELD TRAINING ADMINISTRATOR

The Field Training Administrator will review and approve the Daily Trainee Performance Evaluations submitted by the FTO through the assigned immediate supervisor.

416.6.4 TRAINEE

At the completion of the Field Training Program, the trainee shall submit a confidential performance evaluation on each of their FTOs and on the Field Training Program.

416.7 DOCUMENTATION

All documentation of the Field Training Program will be retained in the officer's training files and will consist of the following:

- (a) Daily Trainee Performance Evaluations.
- (b) End of phase evaluations.
- (c) A Certificate of Completion certifying that the trainee has successfully completed the required number of hours of field training.
- (d) All in-house, specific training, and total training hours shall be submitted to the training coordinator to enter into the State of Utah Training Portal.

Obtaining Air Support

417.1 PURPOSE AND SCOPE

The use of a law enforcement helicopter can be invaluable in certain situations. This policy specifies potential situations where the use of a helicopter may be requested and the responsibilities for making a request.

417.2 REQUEST FOR HELICOPTER ASSISTANCE

If a supervisor or officer in charge of an incident determines that the use of a helicopter would be beneficial, a request to obtain helicopter assistance may be made.

417.2.1 REQUEST FOR ASSISTANCE FROM ANOTHER AGENCY

After consideration and approval of the request for a helicopter, the Watch Commander, or designee, will call the closest agency having helicopter support available. The Watch Commander will apprise that agency of the specific details of the incident prompting the request.

417.2.2 CIRCUMSTANCES UNDER WHICH AID MAY BE REQUESTED

Law enforcement helicopters may be requested under any of the following conditions:

- (a) When the helicopter is activated under existing mutual aid agreements.
- (b) Whenever the safety of law enforcement personnel is in jeopardy and the presence of the helicopters may reduce such hazard.
- (c) When the use of the helicopters will aid in the capture of a suspected fleeing felon whose continued freedom represents an ongoing threat to the community.
- (d) When a helicopter is needed to locate a person who has strayed or is lost and whose continued absence constitutes a serious health or safety hazard.
- (e) Vehicle pursuits.

While it is recognized that the availability of helicopter support will generally provide valuable assistance to ground personnel, the presence of a helicopter will rarely replace the need for officers on the ground.

Contacts and Temporary Detentions

418.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for temporarily detaining but not arresting persons in the field, conducting field interviews (FI) and pat-down searches, and the taking and disposition of photographs.

418.1.1 DEFINITIONS

Definitions related to this policy include:

Consensual encounter - When an officer contacts an individual but does not create a detention through words, actions, or other means. In other words, a reasonable individual would believe that his/her contact with the officer is voluntary.

Field interview (FI) - The brief detainment of an individual, whether on foot or in a vehicle, based on reasonable suspicion for the purposes of determining the individual's identity and resolving the officer's suspicions.

Field photographs - Posed photographs taken of a person during a contact, temporary detention, or arrest in the field. Undercover surveillance photographs of an individual and recordings captured by the normal operation of a Mobile Audio/Video (MAV) system, body-worn camera, or public safety camera when persons are not posed for the purpose of photographing are not considered field photographs.

Pat-down search - A type of search used by officers in the field to check an individual for dangerous weapons. It involves a thorough patting-down of clothing to locate any weapons or dangerous items that could pose a danger to the officer, the detainee, or others.

Reasonable suspicion - When, under the totality of the circumstances, an officer has articulable facts that criminal activity may be afoot and a particular person is connected with that possible criminal activity.

Temporary detention - When an officer intentionally, through words, actions, or physical force, causes an individual to reasonably believe he/she is required to restrict his/her movement without an actual arrest. Temporary detentions also occur when an officer actually restrains a person's freedom of movement.

418.2 FIELD INTERVIEWS

Based on observance of suspicious circumstances or upon information from investigation, an officer may initiate the stop of a person, and conduct an FI, when there is articulable, reasonable suspicion to do so. A person, however, shall not be detained longer than is reasonably necessary to resolve the officer's suspicion (Utah Code 77-7-15).

Nothing in this policy is intended to discourage consensual contacts. Frequent casual contact with consenting individuals is encouraged by the South Salt Lake Police Department to strengthen community involvement, community awareness, and problem identification.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Contacts and Temporary Detentions

418.2.1 INITIATING A FIELD INTERVIEW

When initiating the stop, the officer should be able to point to specific facts which, when considered with the totality of the circumstances, reasonably warrant the stop. Such facts include but are not limited to an individual's:

- (a) Appearance or demeanor suggesting that the individual is part of a criminal enterprise or is engaged in a criminal act.
- (b) Actions suggesting that the individual is engaged in a criminal activity.
- (c) Presence in an area at an inappropriate hour of the day or night.
- (d) Presence in a particular area is suspicious.
- (e) Carrying of suspicious objects or items.
- (f) Excessive clothes for the climate or clothes bulging in a manner that suggest the individual is carrying a dangerous weapon.
- (g) Location in proximate time and place to an alleged crime.
- (h) Physical description or clothing worn that matches a suspect in a recent crime.
- (i) Prior criminal record or involvement in criminal activity as known by the officer.

418.3 PAT-DOWN SEARCHES

Once a valid stop has been made, and consistent with the officer's training and experience, an officer may pat a suspect's outer clothing for weapons if the officer has a reasonable, articulable suspicion the suspect may pose a safety risk (Utah Code 77-7-16). The purpose of this limited search is not to discover evidence of a crime, but to allow the officer to pursue the investigation without fear of violence. Circumstances that may establish justification for performing a pat-down search include but are not limited to:

- (a) The type of crime suspected, particularly in crimes of violence where the use or threat of weapons is involved.
- (b) Where more than one suspect must be handled by a single officer.
- (c) The hour of the day and the location or area where the stop takes place.
- (d) Prior knowledge of the suspect's use of force and/or propensity to carry weapons.
- (e) The actions and demeanor of the suspect.
- (f) Visual indications which suggest that the suspect is carrying a firearm or other dangerous weapon.

Whenever practicable, a pat-down search should not be conducted by a lone officer. A cover officer should be positioned to ensure safety and should not be involved in the search.

418.4 FIELD PHOTOGRAPHS

All available databases should be searched before photographing any field detainee. If a photograph is not located, or if an existing photograph no longer resembles the detainee, the officer shall carefully consider, among other things, the factors listed below.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Contacts and Temporary Detentions

418.4.1 FIELD PHOTOGRAPHS TAKEN WITH CONSENT

Field photographs may be taken when the subject being photographed knowingly and voluntarily gives consent. When taking a consensual photograph, the officer should have the individual read and sign the appropriate form accompanying the photograph.

418.4.2 FIELD PHOTOGRAPHS TAKEN WITHOUT CONSENT

Field photographs may be taken without consent only if they are taken during a detention that is based upon reasonable suspicion of criminal activity, and the photograph serves a legitimate law enforcement purpose related to the detention. The officer must be able to articulate facts that reasonably indicate that the subject was involved in or was about to become involved in criminal conduct. The subject should not be ordered to remove or lift any clothing for the purpose of taking a photograph.

If, prior to taking a photograph, the officer's reasonable suspicion of criminal activity has been dispelled, the detention must cease and the photograph should not be taken.

All field photographs and related reports shall be submitted to a supervisor and retained in compliance with this policy.

418.4.3 SUPERVISOR RESPONSIBILITIES

While it is recognized that field photographs often become valuable investigative tools, supervisors should monitor such practices in view of the above listed considerations. This is not to imply that supervisor approval is required before each photograph is taken.

Access to, and use of, field photographs shall be strictly limited to law enforcement purposes.

418.4.4 DISPOSITION OF PHOTOGRAPHS

All detainee photographs must be adequately labeled and submitted to the Watch Commander with either an associated FI card or other documentation explaining the nature of the contact. If an individual is photographed as a suspect in a particular crime, the photograph should be submitted as an evidence item in the related case, following standard evidence procedures.

If a photograph is not associated with an investigation where a case number has been issued, the Watch Commander should review and forward the photograph to one of the following locations:

- (a) If the photograph and associated FI or documentation are relevant to criminal organization/enterprise enforcement, the Watch Commander will forward the photograph and documents to the designated criminal intelligence system supervisor. The supervisor will ensure the photograph and supporting documents are retained as prescribed in the Criminal Organizations Policy.
- (b) Photographs that do not qualify for retention in a criminal intelligence system or temporary information file shall be forwarded to the Records Section.

When a photograph is taken in association with a particular case, the investigator may use such photograph in a photo lineup. Thereafter, the individual photograph should be retained as a part of the case file. All other photographs shall be retained in accordance with the established records retention schedule.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Contacts and Temporary Detentions

418.4.5 NOTICE REQUIREMENT FOR PHOTOS

Prior to taking a photograph, the officer shall notify the individual that their image may be used in conjunction with facial recognition technology, if applicable (Utah Code 77-23e-105). See the Facial Recognition Technology Use Policy for additional guidance.

418.5 POLICY

The South Salt Lake Police Department respects the right of the public to be free from unreasonable searches or seizures. Due to an unlimited variety of situations confronting the officer, the decision to temporarily detain a person and complete an FI, pat-down search, or field photograph shall be left to the officer based on the totality of the circumstances, officer safety considerations, and constitutional safeguards.

418.6 WITNESS IDENTIFICATION AND INTERVIEWS

Because potential witnesses to an incident may become unavailable or the integrity of their statements compromised with the passage of time, officers should, when warranted by the seriousness of the case, take reasonable steps to promptly coordinate with an on-scene supervisor and/or criminal investigator to utilize available members for the following:

- (a) Identify all persons present at the scene and in the immediate area.
 - 1. When feasible, a recorded statement should be obtained from those who claim not to have witnessed the incident but who were present at the time it occurred.
 - 2. Any potential witness who is unwilling or unable to remain available for a formal interview should not be detained absent reasonable suspicion to detain or probable cause to arrest. Without detaining the individual for the sole purpose of identification, officers should attempt to identify the witness prior to the witness's departure.
- (b) Witnesses who are willing to provide a formal interview should be asked to meet at a suitable location where criminal investigators may obtain a recorded statement. Such witnesses, if willing, may be transported by [department/office] members.
 - 1. A written, verbal, or recorded statement of consent should be obtained prior to transporting a witness. When the witness is a minor, consent should be obtained from the parent or guardian, if available, prior to transport.

418.7 PORTABLE BIOMETRIC CAPTURE DEVICES

Officers assigned to duties outside of [department/office] facilities shall be supplied a portable biometric capture device while on-duty to assist in identifying suspects and witnesses (Utah Code 53-25-802).

Criminal Organizations

419.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure that the South Salt Lake Police Department appropriately utilizes criminal intelligence systems and temporary information files to support investigations of criminal organizations and enterprises.

419.1.1 DEFINITIONS

Definitions related to this policy include:

Criminal intelligence system - Any record system that receives, stores, exchanges or disseminates information that has been evaluated and determined to be relevant to the identification of a criminal organization or enterprise, its members or affiliates. This does not include temporary information files.

419.2 POLICY

The South Salt Lake Police Department recognizes that certain criminal activities, including but not limited to gang crimes and drug trafficking, often involve some degree of regular coordination and may involve a large number of participants over a broad geographical area.

It is the policy of this [department/office] to collect and share relevant information while respecting the privacy and legal rights of the public.

419.3 CRIMINAL INTELLIGENCE SYSTEMS

No [department/office] member may create, submit to, or obtain information from a criminal intelligence system unless the Chief of Police has approved the system for [department/office] use.

Any criminal intelligence system approved for [department/office] use should meet or exceed the standards of 28 CFR 23.20.

A designated supervisor will be responsible for maintaining each criminal intelligence system that has been approved for [department/office] use. The supervisor or the authorized designee should ensure the following:

- (a) Members using any such system are appropriately selected and trained.
- (b) Use of every criminal intelligence system is appropriately reviewed and audited.
- (c) Any system security issues are reasonably addressed.

419.3.1 SYSTEM ENTRIES

It is the designated supervisor's responsibility to approve the entry of any information from a report, FI, photo, or other relevant document into an authorized criminal intelligence system. If entries are made based upon information that is not on file with this [department/office], such as open or public source documents or documents that are on file at another agency, the designated supervisor should ensure copies of those documents are retained by the Records Section. Any supporting documentation for an entry shall be retained by the Records Section in accordance

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Criminal Organizations

with the established records retention schedule and for at least as long as the entry is maintained in the system.

The designated supervisor should ensure that any documents retained by the Records Section are appropriately marked as intelligence information. The Records Supervisor may not purge such documents without the approval of the designated supervisor.

419.4 TEMPORARY INFORMATION FILE

No member may create or keep files on individuals that are separate from the approved criminal intelligence system. However, members may maintain temporary information that is necessary to actively investigate whether a person or group qualifies for entry into the [department/office]-approved criminal intelligence system (CIS) only as provided in this section. Once information qualifies for inclusion, it should be submitted to the supervisor responsible for consideration of CIS entries.

419.5 INFORMATION RECOGNITION

[Department/Office] members should document facts that suggest an individual, organization, or enterprise is involved in criminal activity and should forward that information appropriately. Examples include but are not limited to:

- (a) Gang indicia associated with a person or residence.
- (b) Information related to a drug-trafficking operation.
- (c) Vandalism indicating an animus for a particular group.
- (d) Information related to an illegal gambling operation.

[Department/Office] supervisors who utilize an authorized criminal intelligence system should work with the Training Coordinator to train members to identify information that may be particularly relevant for inclusion.

419.6 RELEASE OF INFORMATION

[Department/Office] members shall comply with the rules of an authorized criminal intelligence system regarding inquiries and release of information.

Information from a temporary information file may only be furnished to [department/office] members and other law enforcement agencies on a need-to-know basis and consistent with the Records Maintenance and Release Policy.

When an inquiry is made by the parent or guardian of a juvenile as to whether that juvenile's name is in a temporary information file, such information should be provided by the supervisor responsible for the temporary information file, unless there is good cause to believe that the release of such information might jeopardize an ongoing criminal investigation.

419.7 CRIMINAL STREET GANGS

The Investigations Division supervisor should ensure that there are an appropriate number of [department/office] members who can:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Criminal Organizations

- (a) Testify as experts on matters related to criminal street gangs and maintain an above average familiarity with identification of criminal street gangs, criminal street gang members, and patterns of criminal gang activity, as described in Utah Code 76-9-802 et seq. and Utah Code 53-25-601 et seq.
- (b) Coordinate with other agencies in the region regarding criminal street gang crimes and information.
- (c) Train other members to identify gang indicia and investigate criminal street gang-related crimes (Utah Code 53-25-602).

419.8 TRAINING

The Training Coordinator should provide training on best practices in the use of each authorized criminal intelligence system to those tasked with investigating criminal organizations and enterprises. Training should include:

- (a) The protection of civil liberties.
- (b) Participation in a multiagency criminal intelligence system.
- (c) Submission of information into a multiagency criminal intelligence system or the receipt of information from such a system, including any governing federal and state rules and statutes.
- (d) The type of information appropriate for entry into a criminal intelligence system or temporary information file.
- (e) The review and purging of temporary information files.

419.9 GANG LOITERING

Officers may only order suspected gang members to disperse under Utah Code 76-9-903 (prohibiting gang loitering) in the following instances:

- (a) Supervisor approval is granted, or
- (b) The officer has received department-approved gang enforcement training and has been authorized by the Gang Supervisor to enforce this section.

If enforcement action is taken under this section, officers must articulate the reasonable belief that the subjects ordered to disperse are gang members. A supervisor's approval is required for any arrest for failure to disperse.

Officers may not order anyone to disperse under this section for engaging in constitutionally protected, collective advocacy activities (demonstrations), or merely because the officer or a citizen claims offense from the speech or expression of the individuals involved or has personal animosity for the people involved. The officer must articulate that the people were remaining in one place under circumstances that would cause a reasonable belief that the purpose or effect of the loitering was to enable or facilitate a criminal street gang to:

- Establish control over one or more identifiable areas.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Criminal Organizations

- Intimidate others from entering those areas.
- Conceal illegal activities.

Watch Commanders

420.1 PURPOSE AND SCOPE

Each patrol shift must be directed by supervisors who are capable of making decisions and communicating in a manner consistent with Department policies, procedures, practices, functions and objectives. To accomplish this goal, a Lieutenant heads each watch.

420.2 WATCH COMMANDER ROLES AND RESPONSIBILITIES

The role of the Police Watch Commander is pivotal in overseeing and leading the efficient operations of the South Salt Lake Police.

RESPONSIBILITIES: not all inclusive

- (a) Supervise sergeants and officers to ensure compliance with department policies and procedures.
- (b) Ensure sergeants are deployed to cover areas of responsibility based on need and priority.
- (c) Monitor sergeants and officers for professional conduct and effectiveness in handling calls for service.
- (d) Ensure prompt and effective response to priority calls for service,
- (e) Direct response to critical incidents and coordinate the response to ensure safety and efficiency.
- (f) Sign out on scenes either by MDT or through dispatch.
- (g) Conduct random and periodic reviews of reports, to ensure completeness, accuracy and adherence to department standards.
- (h) Ensure all required reports are submitted timely and all necessary follow-up actions are documented
- (i) Ensure sergeants are informed of pertinent critical incidents, training needs, operational needs and proper procedural functions.
- (j) Ensure sergeants conduct monthly inspections.
- (k) Coach sergeants in supporting officers.
- (l) Support sergeant and officers in resolving conflict or concerns that may affect performance or morale.
- (m) Attend briefings and provide emerging training topics, address tactical and/or equipment needs.
- (n) Collaborate with sergeant to plan proactive community policing activities based on crime trends and operational needs at a minimum quarterly and send report to the deputy chief..
- (o) Handle specialty assignments by providing direction, encouraging collaboration and ensuring proper documentation of training, call outs, any injuries, use of force, budgets, accidents and/or other requirements.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Watch Commanders

- (p) Provide timely notifications of critical and/or major incidents to Deputy Chief and Chief of Police via text and/or call.
- (q) Complete Significant Incident Report before end of shift with all pertinent details and email to all the administrative commanders.
- (r) Other duties as assigned to complete the mission of the South Salt Lake Police Department.

420.3 WATCH COMMANDER SCHEDULE

The Watch Commander's shifts are 1400-0000 hours. Watch commanders are required to have lieutenant coverage for Thursday, Friday, Saturday and Sunday shifts. Adjustments to assigned schedule must have prior approval from the Deputy Chief. Watch Commanders should sign on and off duty either by the MDT or through radio transmission to dispatch/VECC.

420.3.1 DESIGNATION AS ACTING WATCH COMMANDER

When a Watch Commander is unavailable for duty Monday-Wednesday and/or during portions of graveyard shifts, in most instances, the senior qualified sergeant shall be designated as the acting Watch Commander. This policy does not preclude designating a less senior sergeant as an acting Watch Commander.

Mobile Audio Video

421.1 PURPOSE AND SCOPE

The South Salt Lake Police Department has equipped marked patrol cars with Mobile Audio Video (MAV) recording systems to provide records of events and assist officers in the performance of their duties. This policy provides guidance on the use of these systems.

421.1.1 DEFINITIONS

Definitions related to this policy include:

Activate - Any process that causes the MAV system to transmit or store video or audio data in an active mode.

In-car camera system and Mobile Audio Video (MAV) system - Synonymous terms which refer to any system that captures audio and video signals, that is capable of installation in a vehicle, and that includes at minimum, a camera, microphone, recorder and monitor.

MAV technician - Personnel certified or trained in the operational use and repair of MAVs, duplicating methods, storage and retrieval methods and procedures, and who have a working knowledge of video forensics and evidentiary procedures.

Recorded media - Audio-video signals recorded or digitally stored on a storage device or portable media.

421.2 POLICY

It is the policy of the South Salt Lake Police Department to use mobile audio and video technology to more effectively fulfill the department's mission and to ensure these systems are used securely and efficiently.

421.3 OFFICER RESPONSIBILITIES

Prior to going into service, each officer will properly equip him/herself to record audio and video in the field. At the end of the shift, each officer will follow the established procedures for providing to the Department any recordings or used media and any other related equipment. Each officer should have adequate recording media for the entire duty assignment. In the event an officer works at a remote location and reports in only periodically, additional recording media may be issued. Only South Salt Lake Police Department identified and labeled media with tracking numbers is to be used.

At the start of each shift, officers should test the MAV system's operation in accordance with manufacturer specifications and department operating procedures and training.

System documentation is accomplished by the officer recording his/her name, serial number, badge or PIN number and the current date and time at the start and again at the end of each shift. If the system is malfunctioning, the officer shall take the vehicle out of service unless a supervisor requests the vehicle remain in service.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Mobile Audio Video

421.4 ACTIVATION OF THE MAV

The MAV system is designed to turn on whenever the unit's emergency lights are activated. The system remains on until it is turned off manually. The audio portion is independently controlled and should be activated manually by the officer whenever appropriate. When audio is being recorded, the video will also record.

421.4.1 REQUIRED ACTIVATION OF MAV

This policy is not intended to describe every possible situation in which the MAV system may be used, although there are many situations where its use is appropriate. An officer may activate the system any time the officer believes it would be appropriate or valuable to document an incident.

In some circumstances it is not possible to capture images of the incident due to conditions or the location of the camera. However, the audio portion can be valuable evidence and is subject to the same activation requirements as the MAV. The MAV system should be activated in any of the following situations:

- (a) All field contacts involving actual or potential criminal conduct, within video or audio range:
 - 1. Traffic stops (to include, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops)
 - 2. Priority responses
 - 3. Vehicle pursuits
 - 4. Suspicious vehicles
 - 5. Arrests
 - 6. Vehicle searches
 - 7. Physical or verbal confrontations or use of force
 - 8. Pedestrian checks
 - 9. DUI investigations including field sobriety tests
 - 10. Consensual encounters
 - 11. Crimes in progress
 - 12. Responding to an in-progress call
- (b) All self-initiated activity in which an officer would normally notify Dispatch
- (c) Any call for service involving a crime where the recorder may aid in the apprehension and/or prosecution of a suspect:
 - 1. Domestic violence calls
 - 2. Disturbance of peace calls

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Mobile Audio Video

3. Offenses involving violence or weapons
 - (d) Any other contact that becomes adversarial after the initial contact, in a situation that would not otherwise require recording
 - (e) Any other circumstance where the officer believes that a recording of an incident would be appropriate

421.4.2 CESSATION OF RECORDING

Once activated, the MAV system should remain on until the incident has concluded. For purposes of this section, conclusion of an incident has occurred when all arrests have been made, arrestees have been transported and all witnesses and victims have been interviewed. Recording may cease if an officer is simply waiting for a tow truck or a family member to arrive, or in other similar situations.

421.4.3 WHEN ACTIVATION IS NOT REQUIRED

Activation of the MAV system is not required when exchanging information with other officers or during breaks, lunch periods, when not in service or actively on patrol.

No member of this department may surreptitiously record a conversation of any other member of this department except with a court order or when lawfully authorized by the Chief of Police or the authorized designee for the purpose of conducting a criminal or administrative investigation.

421.4.4 SUPERVISOR RESPONSIBILITIES

Supervisors should determine if vehicles with non-functioning MAV systems should be placed into service. If these vehicles are placed into service, the appropriate documentation should be made, including notification of Dispatch.

At reasonable intervals, supervisors should validate that:

- (a) Beginning and end-of-shift recording procedures are followed.
- (b) Logs reflect the proper chain of custody, including:
 1. The tracking number of the MAV system media.
 2. The date it was issued.
 3. The law enforcement operator or the vehicle to which it was issued.
 4. The date it was submitted.
 5. Law enforcement operators submitting the media.
 6. Holds for evidence indication and tagging as required.
- (c) The operation of MAV systems by new employees is assessed and reviewed no less than biweekly.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Mobile Audio Video

When an incident arises that requires the immediate retrieval of the recorded media (e.g., serious crime scenes, officer-involved shootings, department-involved collisions), a supervisor shall respond to the scene and ensure that the appropriate supervisor, MAV technician or crime scene investigator properly retrieves the recorded media. The media may need to be treated as evidence and should be handled in accordance with current evidence procedures for recorded media.

Supervisors may activate the MAV system remotely to monitor a developing situation, such as a chase, riot or an event that may threaten public safety, officer safety or both, when the purpose is to obtain tactical information to assist in managing the event. Supervisors shall not remotely activate the MAV system for the purpose of monitoring the conversations or actions of an officer.

421.5 REVIEW OF MAV RECORDINGS

All recording media, recorded images and audio recordings are the property of the Department. Dissemination outside of the agency is strictly prohibited, except to the extent permitted or required by law.

To prevent damage to, or alteration of, the original recorded media, it shall not be copied, viewed or otherwise inserted into any device not approved by the department MAV technician or forensic media staff. When reasonably possible, a copy of the original media shall be used for viewing (unless otherwise directed by the courts) to preserve the original media.

Recordings may be reviewed in any of the following situations:

- (a) For use when preparing reports or statements
- (b) By a supervisor investigating a specific act of officer conduct or for quality assurance
- (c) By a supervisor to assess officer performance
- (d) To assess proper functioning of MAV systems
- (e) By a department investigator, after approval of a supervisor, who is participating in an official investigation, such as a personnel complaint, administrative inquiry or a criminal investigation
- (f) By department personnel who request to review recordings
- (g) By an officer who is captured on or referenced in the video or audio data and reviews and uses such data for any purpose relating to his/her employment
- (h) By court personnel through proper process or with permission of the Chief of Police or the authorized designee
- (i) By the media through proper process or with permission of the Chief of Police or the authorized designee
- (j) To assess possible training value

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Mobile Audio Video

- (k) Recordings may be shown for training purposes. If an involved officer objects to showing a recording, his/her objection will be submitted to the staff to determine if the training value outweighs the officer's objection

Employees desiring to view any previously uploaded or archived MAV recording should submit a request in writing to the Watch Commander. Approved requests should be forwarded to the MAV technician for processing.

In no event shall any recording be used or shown for the purpose of ridiculing or embarrassing any employee.

421.5.1 DIGITAL VIDEO REVIEW

Once recordings are downloaded to the department server, only sergeants and above will have the ability to review digital video on their desk top computers.

421.6 DOCUMENTING MAV USE

If any incident is recorded with either the video or audio system, the existence of that recording shall be documented in the officer's report. If a citation is issued, the officer shall make a notation on the back of the records copy of the citation indicating that the incident was recorded.

421.7 RECORDING MEDIA STORAGE AND INTEGRITY

Once submitted for storage, all recording media will be labeled and stored in a designated secure area. All recording media that is not booked as evidence will be retained for a minimum of 180 days and disposed of in compliance with the established records retention schedule.

421.7.1 COPIES OF ORIGINAL RECORDING MEDIA

Original recording media shall not be used for any purpose other than for initial review by a supervisor. Upon proper request, a copy of the original recording media will be made for use as authorized in this policy.

Original recording media may only be released in response to a court order or upon approval by the Chief of Police or the authorized designee. In the event that an original recording is released to a court, a copy shall be made and placed in storage until the original is returned.

421.7.2 MAV RECORDINGS AS EVIDENCE

Officers who reasonably believe that a MAV recording is likely to contain evidence relevant to a criminal offense, potential claim against the officer or against the South Salt Lake Police Department should indicate this in an appropriate report. Officers should ensure relevant recordings are preserved.

421.8 SYSTEM OPERATIONAL STANDARDS

- (a) MAV system vehicle installations should be based on officer safety requirements and the vehicle and device manufacturer's recommendations.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Mobile Audio Video

- (b) The MAV system should be configured to minimally record for 30 seconds prior to an event.
- (c) The MAV system may not be configured to record audio data occurring prior to activation.
- (d) Unless the transmitters being used are designed for synchronized use, only one transmitter, usually the primary initiating officer's transmitter, should be activated at a scene to minimize interference or noise from other MAV transmitters.
- (e) Officers using digital transmitters that are synchronized to their individual MAV shall activate both audio and video recordings when responding in a support capacity. This is to obtain additional perspectives of the incident scene.
- (f) With the exception of law enforcement radios or other emergency equipment, other electronic devices should not be used inside MAV-equipped law enforcement vehicles to minimize the possibility of causing electronic or noise interference with the MAV system.
- (g) Officers shall not erase, alter, reuse, modify or tamper with MAV recordings. Only a supervisor, MAV technician or other authorized designee may erase and reissue previous recordings and may only do so pursuant to the provisions of this policy.
- (h) To prevent damage, original recordings shall not be viewed on any equipment other than the equipment issued or authorized by the MAV technician.

421.9 MAV TECHNICIAN RESPONSIBILITIES

The MAV technician is responsible for:

- (a) Ordering, issuing, retrieving, storing, erasing and duplicating of all recorded media.
- (b) Collecting all completed media for oversight and verification of wireless downloaded media. Once collected, the MAV technician:
 - 1. Ensures it is stored in a secure location with authorized controlled access.
 - 2. Makes the appropriate entries in the chain of custody log.
- (c) Erasing of media:
 - 1. Pursuant to a court order.
 - 2. In accordance with established records retention policies, including reissuing all other media deemed to be of no evidentiary value.
- (d) Assigning all media an identification number prior to issuance to the field:
 - 1. Maintaining a record of issued media.
- (e) Ensuring that an adequate supply of recording media is available.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Mobile Audio Video

- (f) Managing the long-term storage of media that has been deemed to be of evidentiary value in accordance with the department evidence storage protocols and the records retention schedule.

421.10 TRAINING

All members who are authorized to use the MAV system shall successfully complete an approved course of instruction prior to its use.

Mobile Data Terminal Use

422.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the proper access, use, and application of the Mobile Data Terminal (MDT) system in order to ensure appropriate access to confidential records from local, state, and national law enforcement databases, and to ensure effective electronic communications between [department/office] members and Dispatch. See the CJIS Access, Maintenance, and Security Policy for additional guidance.

422.2 POLICY

South Salt Lake Police Department members using the MDT shall comply with all appropriate federal and state rules and regulations and shall use the MDT in a professional manner, in accordance with this policy.

422.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to messages accessed, transmitted, received, or reviewed on any [department/office] technology system (see the Information Technology Use Policy for additional guidance).

422.4 RESTRICTED ACCESS AND USE

MDT use is subject to the Information Technology Use, Protected Information, and CJIS Access, Maintenance, and Security policies.

Members shall not access the MDT system if they have not received prior authorization and the required training. Members shall immediately report unauthorized access or use of the MDT by another member to their supervisors or Watch Commanders.

Use of the MDT system to access law enforcement databases or transmit messages is restricted to official activities, business-related tasks, and communications that are directly related to the business, administration, or practices of the [Department/Office]. In the event that a member has questions about sending a particular message or accessing a particular database, the member should seek prior approval from their supervisor.

Sending derogatory, defamatory, obscene, disrespectful, sexually suggestive, harassing, or any other inappropriate messages on the MDT system is prohibited and may result in discipline.

It is a violation of this policy to transmit a message or access a law enforcement database under another member's name or to use the password of another member to log in to the MDT system unless directed to do so by a supervisor. Members are required to log off the MDT or secure the MDT when it is unattended. This added security measure will minimize the potential for unauthorized access or misuse.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Mobile Data Terminal Use

422.4.1 USE WHILE DRIVING

Use of the MDT by the vehicle operator should be limited to times when the vehicle is stopped. Information that is required for immediate enforcement, investigative, tactical or safety needs should be transmitted over the radio.

In no case shall an operator attempt to send or review lengthy messages while the vehicle is in motion.

422.5 DOCUMENTATION OF ACTIVITY

Except as otherwise directed by the Watch Commander or other [department/office]-established protocol, all calls for service assigned by a dispatcher should be communicated by voice over the police radio and electronically via the MDT unless security or confidentiality prevents such broadcasting.

MDT and voice transmissions are used to document the member's daily activity. To ensure accuracy:

- (a) All contacts or activity shall be documented at the time of the contact.
- (b) Whenever the activity or contact is initiated by voice, it should be documented by a dispatcher.
- (c) Whenever the activity or contact is not initiated by voice, the member shall document it via the MDT.

422.5.1 STATUS CHANGES

All changes in status (e.g., arrival at scene, meal periods, in service) will be transmitted over the police radio or through the MDT system.

Members responding to in-progress calls should advise changes in status over the radio to assist other members responding to the same incident. Other changes in status can be made on the MDT when the vehicle is not in motion.

422.5.2 EMERGENCY ACTIVATION

If there is an emergency activation and the member does not respond to a request for confirmation of the need for emergency assistance or confirms the need, available resources will be sent to assist in locating the member. If the location is known, the nearest available officer should respond in accordance with the Officer Response to Calls Policy.

Members should ensure a field supervisor and the Watch Commander are notified of the incident without delay.

Officers not responding to the emergency shall refrain from transmitting on the police radio until a no-further-assistance broadcast is made or if they are also handling an emergency.

Portable Audio/Video Recorders

423.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of portable audio/video recording devices by members of this [department/office] while in the performance of their duties. Portable audio/video recording devices include all recording systems whether body-worn, handheld, or integrated into portable equipment (Utah Code 77-7a-102).

This policy does not apply to mobile audio/video recordings, interviews, or interrogations conducted at any South Salt Lake Police Department facility, or to wiretaps or eavesdropping (concealed listening devices). Except to the extent provided in Utah Code 77-7a-104, this policy does not apply to officers engaged in undercover operations or assigned to a narcotics unit or a task force engaged primarily in narcotics investigations.

Additional guidance regarding the use of body-worn cameras during the execution of a warrant is found in the Warrant Service Policy.

423.2 POLICY

The South Salt Lake Police Department may provide members with access to portable recorders, either audio or video or both, for use during the performance of their duties. The use of recorders is intended to enhance the mission of the Department by accurately capturing contacts between members of the Department and the public.

423.3 MEMBER PRIVACY EXPECTATION

All recordings made by members on any department-issued device at any time, and any recording made while acting in an official capacity of this department, regardless of ownership of the device it was made on, shall remain the property of the Department. Members shall have no expectation of privacy or ownership interest in the content of these recordings.

All portable recorders, will not be allowed in locker room or restroom areas. Members shall not surreptitiously record any member in the locker room or restroom areas.

423.4 MEMBER RESPONSIBILITIES

Prior to going into service, each uniformed member will be responsible for making sure that he/she is equipped with a portable recorder issued by the Department, and that the recorder is in good working order. If the recorder is not in working order or the member becomes aware of a malfunction at any time, the member shall promptly report the failure to his/her supervisor and obtain a functioning device as soon as reasonably practicable. Uniformed members should wear the recorder in a conspicuous manner or otherwise notify persons that they are being recorded, whenever reasonably practicable (Utah Code 77-7a-104; Utah Code 77-7a-105).

Any member assigned to a non-uniformed position may carry an approved portable recorder at any time the member believes that such a device may be useful. Unless conducting a lawful recording in an authorized undercover capacity, non-uniformed members should wear the recorder in a

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Portable Audio/Video Recorders

conspicuous manner when in use or otherwise notify persons that they are being recorded, whenever reasonably practicable.

When using a portable recorder, the assigned member shall record his/her name, SSLPD identification number and the current date and time at the beginning and the end of the shift or other period of use, regardless of whether any activity was recorded. This procedure is not required when the recording device and related software captures the user's unique identification and the date and time of each recording (Utah Code 77-7a-104).

Members should document the existence of a recording in any report or other official record of the contact, including any instance where the recorder malfunctioned or the member deactivated the recording. Members should include the reason for deactivation (Utah Code 77-7a-104).

It is the members responsibility to have a BWC worn and activated per state law, SSLPD policies and during department approved off-duty/outside employment.

423.5 SUPERVISOR RESPONSIBILITIES

Supervisors have a responsibility to ensure policies and proper procedures are adhered to while officers are utilizing the portable audio/video recorders. Supervisors should review portable audio/video recorders to investigate specific acts of employee conduct, review for accuracy of reports or assist in writing a report, and/or proper submission of evidence.

Supervisors are prohibited from conducting random and/or curiosity reviews of portable recorders/video recorders.

423.6 ACTIVATION OF THE PORTABLE RECORDER

This policy is not intended to describe every possible situation in which the portable recorder should be used, although there are many situations where its use is appropriate. Members should activate the recorder any time the member believes it would be appropriate or valuable to record an incident.

The portable recorder shall be activated in any of the following situations (Utah Code 77-7a-103; Utah Code 77-7a-104):

- (a) All enforcement and investigative contacts including stops and field interview situations
- (b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops
- (c) Self-initiated activity in which a member would normally notify Dispatch
- (d) Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require recording
- (e) Any use of force
- (f) Dispatched calls for service
- (g) Execution of a warrant

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Portable Audio/Video Recorders

Members should remain sensitive to the dignity of all individuals being recorded and exercise sound discretion to respect privacy by discontinuing recording whenever it reasonably appears to the member that such privacy may outweigh any legitimate law enforcement interest in recording. Requests by members of the public to stop recording should be considered using this same criterion. Recording should resume when privacy is no longer at issue unless the circumstances no longer fit the criteria for recording.

At no time is a member expected to jeopardize his/her safety in order to activate a portable recorder or change the recording media (Utah Code 77-7a-102). However, the recorder should be activated in situations described above as soon as reasonably practicable (Utah Code 77-7a-104).

423.6.1 SURREPTITIOUS USE OF THE PORTABLE RECORDER

Utah law permits an individual to surreptitiously record any conversation in which one party to the conversation has given his/her permission (Utah Code 77-23a-4).

Members of the Department may surreptitiously record any conversation during the course of a criminal investigation in which the member reasonably believes that such a recording will be lawful and beneficial to the investigation.

Members shall not surreptitiously record another department member without a court order unless lawfully authorized by the Chief of Police or the authorized designee.

423.6.2 CESSATION OF RECORDING

Once activated, the portable recorder should remain on continuously until the member reasonably believes his/her direct participation in the incident is complete or the situation no longer fits the criteria for activation. Recording may be stopped (Utah Code 77-7a-104):

- (a) During significant periods of inactivity such as report writing or other breaks from direct participation in the incident, including consultation with a supervisor or other officer.
- (b) When speaking with a victim, witness, or person wishing to report or discuss criminal activity if both of the following apply:
 - 1. The subject of the recording requests deactivation.
 - 2. The member believes the value of the information outweighs the value of the potential recording.
- (c) During a conversation with a victim of a sexual offense or domestic violence if:
 - 1. The member is conducting an evidence-based lethality assessment.
 - 2. The victim or the member believes that deactivating the body-worn camera recording will either:
 - (a) Encourage complete and accurate information sharing by the victim, or
 - (b) Is necessary to protect the safety or identity of the victim.
 - 3. The body-worn camera is reactivated as soon as reasonably possible after the evidence-based lethality assessment is complete.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Portable Audio/Video Recorders

The member should record the request to deactivate the portable recorder. A member should document any instance where he/she should have activated his/her body-worn camera but failed to do so, and the reason for the failure (Utah Code 77-7a-104).

423.6.3 EXPLOSIVE DEVICE

Many portable recorders, including body-worn cameras and audio/video transmitters, emit radio waves that could trigger an explosive device. Therefore, these devices should not be used where an explosive device may be present.

423.7 PROHIBITED USE OF PORTABLE RECORDERS

Members are prohibited from using department-issued portable recorders and recording media for personal use and are prohibited from making personal copies of recordings created while on-duty or while acting in their official capacity. Members may not alter or delete a recording captured on a portable recorder (Utah Code 77-7a-106).

Members are also prohibited from retaining recordings of activities or information obtained while on-duty whether the recording was created with a department-issued or personally owned recorder. Members shall not duplicate or distribute such recordings, except for authorized legitimate department business purposes. All such recordings shall be retained at the Department (Utah Code 77-7a-106).

Members are prohibited from using personally owned recording devices while on-duty without the express consent of the Watch Commander. Any member who uses a personally owned recorder for department-related activities shall comply with the provisions of this policy, including retention and release requirements, and should notify the on-duty supervisor of such use as soon as reasonably practicable.

Recordings shall not be used by any member for the purpose of embarrassment, harassment or ridicule.

423.8 IDENTIFICATION AND PRESERVATION OF RECORDINGS

To assist with identifying and preserving data and recordings members should download, tag or mark these in accordance with procedure and document the existence of the recording in any related case report.

A member should transfer, tag or mark recordings when the member reasonably believes:

- (a) The recording contains evidence relevant to potential criminal, civil or administrative matters.
- (b) A complainant, victim or witness has requested non-disclosure.
- (c) A complainant, victim or witness has not requested non-disclosure but the disclosure of the recording may endanger the person.
- (d) Disclosure may be an unreasonable violation of someone's privacy.
- (e) Medical or mental health information is contained.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Portable Audio/Video Recorders

- (f) Disclosure may compromise an under-cover officer or confidential informant.
- (g) Recorded content contains sound or images from a residence (Utah Code 63G-2-302).
- (h) Recorded content contains sound or images from a hospital, health care facility, human service program or the clinic of a health care provider (Utah Code 63G-2-305).

Any time a member reasonably believes a recorded contact may be beneficial in a non-criminal matter (e.g., a hostile contact), the member should promptly notify a supervisor of the existence of the recording.

423.9 REVIEW OF RECORDED MEDIA FILES

When preparing written reports, members should review their recordings as a resource (see the Officer-Involved Shootings and Deaths Policy for guidance in those cases). However, members shall not retain personal copies of recordings. Members should not use the fact that a recording was made as a reason to write a less detailed report.

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct or whenever such recordings would be beneficial in reviewing the member's performance.

Recorded files may also be reviewed:

- (a) Upon approval by a supervisor, by any member of the Department who is participating in an official investigation, such as a personnel complaint, administrative investigation or criminal investigation.
- (b) Pursuant to lawful process or by court personnel who are otherwise authorized to review evidence in a related case.
- (c) By media personnel with permission of the Chief of Police or the authorized designee.
- (d) In compliance with a public records request, if permitted, and in accordance with the Records Maintenance and Release Policy.

All recordings should be reviewed by the Custodian of Records prior to public release (see the Records Maintenance and Release Policy). Recordings that unreasonably violate a person's privacy or sense of dignity should not be publicly released unless disclosure is required by law or order of the court.

423.10 COORDINATOR

The Chief of Police or the authorized designee should designate a coordinator responsible for establishing procedures for (Utah Code 77-7a-102):

- (a) The security, storage and maintenance of data and recordings.
- (b) Accessing data and recordings.
- (c) Logging or auditing access.
- (d) Transferring, downloading, tagging or marking events.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Portable Audio/Video Recorders

423.11 RETENTION OF RECORDINGS

All recordings shall be retained for a period consistent with the requirements of the established records retention schedule and as required by any applicable federal, state and local law (Utah Code 77-7a-107).

423.11.1 RELEASE OF AUDIO/VIDEO RECORDINGS

Requests for the release of audio/video recordings shall be processed in accordance with the Records Maintenance and Release Policy.

423.12 PUBLIC ACCESS

The Records Supervisor should ensure that this policy is available to the public in written format as well as published to the department website (Utah Code 77-7a-105).

Bicycle Patrol Unit

424.1 PURPOSE AND SCOPE

The South Salt Lake Police Department has established the Bicycle Patrol Unit (BPU) for the purpose of enhancing patrol efforts in the community. Bicycle patrol has been shown to be an effective way to increase officer visibility in congested areas. The quiet operation of the bicycles also can provide a tactical approach to crimes in progress. The purpose of this policy is to provide guidelines for the safe and effective operation of the patrol bicycle.

424.2 POLICY

Patrol bicycles may be used for regular patrol duty, traffic enforcement, parking control or special events. The use of the patrol bicycle will emphasize officers mobility and visibility to the community.

Bicycles may be deployed to any area at all hours of the day or night, according to Department needs and as staffing levels allow.

Requests for specific deployment of bicycle patrol officers shall be coordinated through the Bicycle Patrol Unit supervisor or the Watch Commander.

424.3 SELECTION OF PERSONNEL

Interested sworn personnel, who are off probation, shall submit a change of assignment request to their appropriate Division Commander. A copy will be forwarded to the BPU supervisor. Qualified applicants will then be invited to an oral interview. The oral board will consist of the BPU supervisor and a second person to be selected by the BPU supervisor. Interested personnel shall be evaluated by the following criteria:

- (a) Recognized competence and ability as evidenced by performance.
- (b) Special skills or training as it pertains to the assignment.
- (c) Good physical condition.
- (d) Willingness to perform duties using the bicycle as a mode of transportation.

424.3.1 BICYCLE PATROL UNIT SUPERVISOR

The Bicycle Patrol Unit supervisor will be selected from the rank of sergeant by the Patrol Division Commander or designee.

The Bicycle Patrol Unit supervisor shall have responsibility for the following:

- (a) Organizing bicycle patrol training.
- (b) Inspecting and maintaining inventory of patrol bicycles and program equipment.
- (c) Scheduling maintenance and repairs.
- (d) Evaluating performance of bicycle officers.
- (e) Coordinating activities with the Patrol Division.
- (f) Other activities as required to maintain the efficient operation of the Bicycle Patrol Unit.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Bicycle Patrol Unit

424.3.2 SCHEDULING

The bike patrol program will run from April 1st through September 30th, weather permitting. Scheduling will be governed and authorized by the team leader on a monthly basis. The schedule will be posted and shifts will be available on a sign up basis. Officers will be encouraged, but not required to ride their bikes while on duty for regular patrol duties. Riding during the shift will be based on shift coverage and with the approval of the shift sergeant.

424.3.3 PERFORMANCE

- (a) Performance and pro-activity are a must for the bike patrol unit.
 - 1. At all times there will be a standard of minimum activity established.
 - 2. This standard may change from year to year based on the needs of the bike patrol unit, the patrol division as well as the agency as a whole.
 - 3. The standard(s) for the year will be addressed and outlined in the annual training and meetings.
- (b) Any Bike Patrol officer who does not ride the required number of hours per month, will be removed from the bike patrol unit.
 - 1. All members of the Bike Unit will be required to meet the performance standards established by the unit supervisor.
 - 2. Special assignments as described in Section 454.7.1 do not count toward time required to ride.

424.4 TRAINING

- (a) All bike patrol officers are required to receive training annually. In addition, all bike patrol officers will be required to attend, and successfully complete a department or P.O.S.T. sponsored Basic Bike Patrol training class.
 - 1. Annual training will consist of at a minimum:
 - (a) Physical fitness.
 - (b) Bike Safety.
 - (c) Community relations.
 - (d) Maintenance.
- (b) Any officer in good standing with the department that has completed a bike patrol training class is authorized to participate in the bike patrol program.
- (c) Bicycle patrol officers will be required to qualify with their duty firearm while wearing bicycle safety equipment including the helmet and riding gloves.

424.5 UNIFORMS AND EQUIPMENT

Officers shall wear the Department-approved uniform and safety equipment while operating the department bicycle. Safety equipment includes Department-approved helmet, riding gloves, protective eyewear and approved footwear.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Bicycle Patrol Unit

The bicycle patrol unit uniform consists of the standard short-sleeve uniform shirt or other department-approved shirt with Department badge and patches and department-approved bicycle patrol pants or shorts.

Optional equipment includes a radio head set and microphone. In colder weather a jacket may be worn.

Bicycle patrol officers shall carry the same equipment on the bicycle patrol duty belt as they would on a regular patrol assignment.

Officers will be responsible for obtaining the necessary forms, citation books and other department equipment needed while on bicycle patrol.

424.6 CARE AND USE OF PATROL BICYCLES

- (a) Officers will be assigned a specially marked and equipped patrol bicycle, attached gear bag, three batteries and a charger.
- (b) Bicycles utilized for uniformed bicycle patrol shall be primarily black or white with a Police decal affixed to each side of the crossbar or the bike's saddlebag. Every such bicycle shall be equipped with front and rear reflectors, front lights and a siren/horn satisfying the requirements of Utah Code 41-6a-1114.
- (c) Bicycles utilized for uniformed bicycle patrol shall be equipped with a rear rack and/or saddle bag(s) sufficient to carry all necessary equipment to handle routine patrol calls, including report writing, vehicle storage and citations.
- (d) Bicycle officers shall conduct an inspection of the bicycle and equipment prior to use to ensure proper working order of the equipment. Officers are responsible for the routine care and maintenance of their assigned equipment (e.g., tire pressure, chain lubrication, overall cleaning).
- (e) If a needed repair is beyond the ability of the bicycle officer, a repair work order will be completed and forwarded to the program supervisor for repair by an approved technician.
- (f) Each bicycle will have scheduled maintenance twice yearly to be performed by a Department-approved repair shop/technician.
- (g) At the end of a bicycle assignment, the bicycle shall be returned clean and ready for the next tour of duty.
- (h) Electric patrol bicycle batteries shall be rotated on the assigned charger at the end of each tour of duty. During prolonged periods of non-use, each officer assigned an electric bicycle shall periodically rotate the batteries on the respective charges to increase battery life.
- (i) Officers shall not modify the patrol bicycle, remove, modify or add components except with the expressed approval of the bicycle supervisor or in the event of an emergency.
- (j) Bicycles shall be properly secured when not in the officer's immediate possession.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Bicycle Patrol Unit

424.7 OFFICER RESPONSIBILITY

Officers must operate the bicycle in compliance with the Utah Code under normal operation. Officers may operate the bicycle without lighting equipment during hours of darkness when such operation reasonably appears necessary for officer safety and tactical considerations. Officers must use caution and care when operating the bicycle without lighting equipment.

Officers are exempt from the rules of the road under the following conditions:

- (a) In response to an emergency call.
- (b) While engaged in rescue operations.
- (c) In the immediate pursuit of an actual or suspected violator of the law.

424.7.1 ACTIVITIES

- (a) In addition to the bike patrol pro-activity standards, bike patrol officers will be required to attend many of the local celebrations and activities. Officers involved in other specialty units may be excused at the discretion of the team leader and sergeant. These activities include but are not limited to:
 - 1. Founders Day Celebration
 - 2. Mural Fest
 - 3. Bike Rodeos
 - 4. Special Olympics Torch Run
 - 5. Craftober Fest
 - 6. Community Night Out
 - 7. Any special event with authorized approval

Foot Pursuits

425.1 PURPOSE AND SCOPE

This policy provides guidelines to assist officers in making the decision to initiate or continue the pursuit of suspects on foot.

425.2 POLICY

It is the policy of the department that officers, when deciding to initiate or continue a foot pursuit, must continuously balance the objective of apprehending the suspect with the risk and potential for injury to department members, the public or the suspect.

Officers are expected to act reasonably, based on the totality of the circumstances.

425.3 DECISION TO PURSUE

The safety of department members and the public should be the primary consideration when determining whether a foot pursuit should be initiated or continued. Officers must be mindful that immediate apprehension of a suspect is rarely more important than the safety of the public and department members.

Officers may be justified in initiating a foot pursuit of any individual that the officer reasonably believes is about to engage in, is engaging in or has engaged in criminal activity. The decision to initiate or continue such a foot pursuit, however, must be continuously re-evaluated in light of the circumstances presented at the time.

Mere flight by a person who is not suspected of criminal activity alone shall not serve as justification for engaging in an extended foot pursuit without the development of reasonable suspicion of the individual's involvement in criminal activity or being wanted by law enforcement.

Deciding to initiate or continue a foot pursuit is a decision that an officer must make quickly and under unpredictable and dynamic circumstances. It is recognized that foot pursuits may place department members and the public at significant risk. Therefore, no officer or supervisor shall be criticized or disciplined for deciding not to engage in a foot pursuit because of the perceived risk involved.

If circumstances permit, surveillance and containment are generally the safest tactics for apprehending fleeing persons. In deciding whether to initiate or continue a foot pursuit, an officer should continuously consider reasonable alternatives to pursuit based upon the circumstances and resources available, such as:

- (a) Containment of the area.
- (b) Saturation of the area with law enforcement personnel, including assistance from other agencies.
- (c) A canine search.
- (d) Thermal imaging or other sensing technology.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Foot Pursuits

- (e) Air support.
- (f) Apprehension at another time when the identity of the suspect is known or there is information available that would likely allow for later apprehension, and the need to immediately apprehend the suspect does not reasonably appear to outweigh the risk of continuing the foot pursuit.

425.4 GENERAL GUIDELINES

When reasonably practicable, officers should consider alternatives to engaging in or continuing a foot pursuit when:

- (a) Directed by a supervisor to terminate the foot pursuit; such an order shall be considered mandatory.
- (b) The officer is acting alone.
- (c) Two or more officers become separated, lose visual contact with one another or obstacles separate them to the degree that they cannot immediately assist each other should a confrontation take place. In such circumstances it is generally recommended that a single officer keep the suspect in sight from a safe distance and coordinate the containment effort.
- (d) The officer is unsure of his/her location and direction of travel.
- (e) The officer is pursuing multiple suspects and it is not reasonable to believe that the officer would be able to control the suspect should a confrontation occur.
- (f) The physical condition of the officer renders him/her incapable of controlling the suspect if apprehended.
- (g) The officer loses radio contact with Dispatch or with backup officers.
- (h) The suspect enters a building, structure, confined space, wooded or otherwise isolated area and there are insufficient officers to provide backup and containment. The primary officer should consider discontinuing the pursuit and coordinate containment, pending the arrival of sufficient resources.
- (i) The officer becomes aware of unanticipated or unforeseen circumstances that unreasonably increase the risk to officers or the public.
- (j) The officer reasonably believes that the danger to the pursuing officers or public outweighs the objective of immediate apprehension.
- (k) The officer loses possession of his/her firearm or other essential equipment.
- (l) The officer or a third party is injured during the pursuit, requiring immediate assistance and there are no other emergency personnel able to render assistance.
- (m) The suspect's location is no longer known.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Foot Pursuits

- (n) The identity of the suspect is established or other information exists that will allow for the suspect's apprehension at a later time and it reasonably appears that there is no immediate threat to department personnel or the public if the suspect is not immediately apprehended.
- (o) The officer's ability to safely continue the pursuit is impaired by inclement weather, darkness, or other conditions.

425.5 RESPONSIBILITIES IN FOOT PURSUITS

425.5.1 INITIATING OFFICER RESPONSIBILITIES

Unless relieved by another officer or a supervisor, the initiating officer shall be responsible for coordinating the progress of the pursuit. When acting alone and when practicable the initiating officer should not attempt to overtake and confront the suspect but should attempt to keep the suspect in sight until sufficient officers are present to safely apprehend the suspect.

Early communication of available information from the involved officers is essential so that adequate resources can be coordinated and deployed to bring a foot pursuit to a safe conclusion. Officers initiating a foot pursuit should broadcast the following information as soon as it becomes practicable and available:

- (a) Location and direction of travel
- (b) Call sign identifier
- (c) Reason for the foot pursuit, such as the crime classification
- (d) Number of suspects and description, to include name if known
- (e) Whether the suspect is known or believed to be armed with a dangerous weapon

Officers should be mindful that radio transmissions made while running may be difficult to understand and may need to be repeated.

Absent extenuating circumstances any officer unable to promptly and effectively broadcast this information should terminate the pursuit. If the foot pursuit is discontinued for any reason, immediate efforts for containment should be established and alternatives considered based upon the circumstances and available resources.

When a foot pursuit terminates, the officer will notify communications with his/her location, the status of the pursuit termination (e.g., suspect in custody, lost sight of suspect) and direct further actions as reasonably appear necessary, to include requesting medical aid as needed for officers, suspects or members of the public.

425.5.2 ASSISTING OFFICER RESPONSIBILITIES

Whenever any officer announces that he/she is engaged in a foot pursuit all other officers should minimize non-essential radio traffic in order to permit the involved officers maximum access to the radio frequency.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Foot Pursuits

425.5.3 SUPERVISOR RESPONSIBILITIES

Upon becoming aware of a foot pursuit, the supervisor shall make every reasonable effort to ascertain sufficient information necessary to direct responding resources and to take command, control and coordination of the foot pursuit. The supervisor should respond to the area whenever possible; the supervisor does not, however, need to be physically present to exercise control over the pursuit. The supervisor shall continuously assess the situation in order to ensure the foot pursuit is conducted within established department guidelines.

The supervisor shall terminate the foot pursuit at any time he/she concludes that the danger to pursuing officers or the public outweighs the objective of immediate apprehension of the suspect.

Upon the apprehension of the suspect the supervisor shall promptly proceed to the termination point to direct the post-pursuit activity.

425.5.4 DISPATCH RESPONSIBILITIES

Upon notification or becoming aware that a foot pursuit is in progress, the dispatcher is responsible for:

- (a) Clearing the radio channel of non-emergency traffic.
- (b) Coordinating pursuit communications of the involved officers.
- (c) Broadcasting pursuit updates as well as other pertinent information as necessary.
- (d) Ensuring that a field supervisor is notified of the foot pursuit.
- (e) Notifying and coordinating with other involved or affected agencies as practicable.
- (f) Notifying the Watch Commander as soon as practicable.
- (g) Assigning an incident number and logging all pursuit activities.

425.6 REPORTING REQUIREMENTS

The initiating officer shall complete appropriate crime/arrest reports documenting, at minimum:

- (a) Date and time of the foot pursuit.
- (b) Initial reason and circumstances surrounding the foot pursuit.
- (c) Course and approximate distance of the foot pursuit.
- (d) Alleged offenses.
- (e) Involved vehicles and officers.
- (f) Whether a suspect was apprehended as well as the means and methods used.
 - 1. Any use of force shall be reported and documented in compliance with the Use of Force Policy.
- (g) Arrestee information, if applicable.
- (h) Any injuries and/or medical treatment.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Foot Pursuits

- (i) Any property or equipment damage.
- (j) Name of the supervisor at the scene or who handled the incident.

Assisting officers taking an active role in the apprehension of the suspect shall complete supplemental reports as necessary or as directed.

The supervisor reviewing the report will make a preliminary determination that the pursuit appears to be in compliance with this policy or that additional review and/or follow-up is warranted.

In any case in which a suspect is not apprehended and there is insufficient information to warrant further investigation, a supervisor may authorize that the initiating officer need not complete a formal report.

Burglary/Intrusion Alarm Response

426.1 PURPOSE AND SCOPE

While burglary/intrusion alarms are often false, it is still incumbent on officers to respond. However, due to the low frequency of these types of alarms being legitimate, the response priority should be low.

The general exception to this rule is when there is additional information related to the alarm that would increase its response priority e.g. independent witnesses reporting a burglary/intrusion, a security patrol that reports suspicious activity or confirms a burglary/intrusion.

In these and similar types of situations the response priority would be elevated based on the specific information provided. Regardless of a burglary/intrusion alarm's low priority, all alarms should be responded to and investigated as call volume allows.

426.1.1 PROCEDURES

- (a) Regardless whether a responsible party or security is responding to an alarm, once VECC has been notified of an alarm Dispatch (VECC) will place the call on the call screen as a priority 3 for the next available officer.
- (b) If, prior to the alarm being dispatched or when the alarm is initially reported, it is determined that a responsible party or security officer has responded and determined there is a problem, the call priority will be raised based on the circumstances reported.
- (c) Once an officer(s) has arrived on scene, made a visual inspection of the location, and determined the alarm appears to be false, the officer may clear the call.
 - 1. If a responsible party is also responding the officer may wait for the responsible party to arrive or, with the supervisors permission may clear the alarm.
 - 2. Officers will, if requested, escort the responsible party when "clearing" the location.
 - 3. It will be the on-duty supervisor's responsibility, based on current call volume and staffing levels, to determine how long the officers may wait for a responsible party to arrive.
- (d) Issues regarding alarm users or alarm central stations will be directed to the on duty patrol sergeant. In the event that the problem/issue cannot be resolved, the issue will be forwarded up the chain of command.
- (e) Excessive false alarms
 - 1. In the event a sergeant or officer becomes aware of an excessive alarm (more than three in a one-month period) at a location, further steps should be taken:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Burglary/Intrusion Alarm Response

- (a) It will be the respective sergeant's responsibility to research the number of false alarms at a location, as well as the reason(s) identified for the false alarms.
 - (b) If the location is a business, the information should be forwarded to "Business Watch" Crime Prevention Officer for follow-up with that business.
 - (c) If the location is residential, the information will be forwarded to the "Neighborhood Watch" Crime Prevention Officer for follow up.
- (f) Reporting
 - (a) Reports related to alarms where a criminal act has occurred must be submitted in accordance with South Salt Lake Police Department Policy, GO1304.
 - (b) When completing a report where officers have been requested at the scene subsequent to burglar/intrusion alarm activation and a crime has occurred, officers are required to enter "ALARM" in the circumstance code of the report so accurate statistical data can be gathered.
 - (c) Officers who respond on robbery, duress or panic alarms that are determined to be false are required to provide the following information to the dispatch notes: the name of the person activating the alarm and a brief statement of the circumstance surrounding the false activation.
 - (d) Officers who respond to a robbery, duress or panic alarm where it is determined that a criminal act has occurred will add "ALARM" to the circumstance code of the report so accurate statistical data can be gathered.

Juvenile Offenders, Contact, Interviews, Interrogation

427.1 PURPOSE AND SCOPE

Contacts with juveniles, in both criminal and non-criminal situations, make up a significant portion of the contacts between the police department and public. Because of this, responsibility for juvenile operations cannot be relegated to a single unit or small group of persons within the police department. Each patrol officer and investigator is accountable for the proper handling of issues related to juveniles within the framework of UCA 62A-4a-201, UCA 62A-4a-202.1 and UCA 78-3a-113.

427.1.1 SCHOOL BASED PROGRAMS

The South Salt Lake City Police Department is committed to the development and maintenance of program to prevent and control juvenile delinquency; such programs include but are not limited to:

- (a) Drug Abuse Resistance Education (DARE).
- (b) School Resource Officers.
- (c) GREAT (Gang Resistance Education and Training).

427.1.2 JUVENILE OFFENDER CONTACT

- (a) When dealing with juvenile offenders, officers of this department will use the least coercive among reasonable alternatives, consistent with preserving order, public safety, and individual liberty. The usual alternatives are:
 - 1. Release on summons for violations of non-felony state traffic laws, fish and game laws, parks and recreation laws or regulations, or municipal ordinances, the penalty for which does include incarceration.
 - 2. Outright release, normally including a verbal warning and may include meeting with parents or guardians, without further action.
 - 3. Temporary custody pursuant to UCA 78-3a-113, with the release to the care of parent or other responsible adult.
 - 4. Release on Summons/Citation.
 - (a) Juveniles who are charged with traffic, violations or other misdemeanor infractions will normally be released on issuance of a citation in lieu of custodial arrest in accordance with UCA 78-3a-503
 - 5. Arrest for DUI and reckless driving will normally coincide with booking. When evidence gathering is complete and the threat of continuing jeopardy is removed, juveniles may be released on citation.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Juvenile Offenders, Contact, Interviews, Interrogation

- (a) Parents or guardians are to be notified and present if practical, in these circumstances.
 - (b) In all cases, the arresting officer will notify parents/guardians as soon as possible.
- (b) When a juvenile fails to sign the traffic infraction, he/she shall be handled in accordance with department policy relating to failure to sign.

427.1.3 JUVENILES IN CUSTODY

- (a) The South Salt Lake City Police Department, in addition to handling juvenile offenders, handles juveniles in crisis (non-criminal). It is the policy of the department to handle these individuals in a manner that establishes trust between the individual and the system, with the primary goal being the protection of the juvenile. Juveniles in crisis will be handled according to the appropriate state statutes and juvenile court rules when taken into custody.
- (b) Status Offender - Cases are governed by UCA 78-3a-117.
 - 1. The South Salt Lake City Police Department will, on notification of a runaway, complete a full report.
 - (a) A copy of the completed approved case will be routed to the investigations supervisor, who will assign the case to an officer if the runaway is still at large.
 - (b) A follow-up investigation will be conducted on each runaway case in logical progression and as soon as practical.
 - 2. "Child At Risk" cases are also governed by UCA 78-3A-113.
 - (a) The South Salt Lake City Police Department will investigate all cases of child abuse or neglect occurring within the city limits.
 - (b) The South Salt Lake City Police Department has a duty by law to notify the Utah State Division of Family Service of all cases of child abuse and / or neglect. This notification shall be made as soon as practical.
 - (c) In accordance with Utah State statute, the reporting officer will, when he/she believes a child(ren) are in continuing jeopardy, immediately involve the Division of Family Services before any child is taken into protective custody.
 - (d) It is the responsibility of the Division of Family Services to facilitate the placement of the child or children into shelter care.
 - (e) UCA 78-3a-113 has very specific requirements and prohibitions for the removal of children from the custody of parents or guardians.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Juvenile Offenders, Contact, Interviews, Interrogation

- (f) Division of Family Services workers should be actively involved in the removal of any child from their parents or guardian.
- (g) All reported incidents require a written report.
 - 1. A copy of each case will be routed to the investigations section that will coordinate or complete follow-up if necessary.
 - 2. It is the responsibility of the investigator assigned the case to ensure that proper notification has been made to the Utah State Division of Family Services.
- 3. Mental illness
 - (a) South Salt Lake City police officers occasionally deal with youths who, without being involved in criminal conduct, are a danger to themselves or others due to their mental state.
 - (b) The department's purpose is to assist in providing immediate professional outreach resources to these individuals.
 - (c) In cases where outreach resources are unavailable and the juvenile is suicidal, officers shall take the juvenile into custody in accordance with UCA 78-3a-113.

427.1.4 TAKING JUVENILES INTO CUSTODY

- (a) The following procedures will be adhered to when taking juveniles into custody (except on school grounds):
 - 1. When arresting a juvenile, the arresting officer should (when practical) immediately advise the juvenile of the offense committed.
 - 2. Prior to conducting an interview, the juvenile should be advised of his/her constitutional rights to include the potential of adult prosecution if the juvenile court declines jurisdiction.
 - (a) If the juvenile is under 14 years of age, his/her parent/guardian must also be advised of Miranda.
 - 3. When available, or as soon as possible after the arrest, the parents/guardian will be notified of the arrest by the arresting officer, or the next shift supervisor, if required.
 - 4. Use of detention rooms for juveniles being detained, refer to South Salt Lake Police Department Policy and Procedure.

427.1.5 INTERVIEW / INTERROGATIONS OF JUVENILES

- (a) Interrogations of juveniles shall be conducted as follows:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Juvenile Offenders, Contact, Interviews, Interrogation

1. A juvenile under the age of 14 shall have parental, guardian, or attorney contact prior to the interview.
 - (a) A minor under 14 years of age may not waive such rights outside of the presence of the minor's parent, guardian or custodian.
2. A juvenile 14 years of age or older, is presumed capable of knowingly and voluntarily waiving their rights without the benefit of a parent, guardian, or legal custodian present during questioning. Utah Rules of Juvenile Procedure 27A (2).
 - (a) A juvenile 14 years of age and older is presumed capable of intelligently comprehending and waiving the minor's right to counsel, and may do so where the court finds such waiver to be knowing and voluntary, whether the minor's parent, guardian or custodian is present.
3. Not more than three officers will be directly involved in an interrogation at any time.
 - (a) The mere presence of three or more officers in a field situation is not prohibited, but when practical, the number of officers should not exceed the number necessary to control the situation at hand.
4. Interrogations should not last longer than is necessary to gain adequate information on the matter of concern.
5. In no case, should an interrogation last longer than three hours without supervisory approval.
6. In such a case, the supervisor should assess the matter with the following factors considered before permitting continuance:
 - (a) Age of juvenile.
 - (b) Location of interview.
 - (c) Maturity level of juvenile.
 - (d) Gravity of offense.
 - (e) Juvenile should be allowed breaks for personal necessities.

Automated License Plate Readers (ALPRs)

428.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained through the use of the automated license plate reader (ALPR) technology (Utah Code 41-6a-2003).

428.2 ADMINISTRATION

The ALPR technology, also known as license plate recognition (LPR), allows for the automated detection of license plates. It is used by the South Salt Lake Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates, and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction, and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access shall be managed by the Administration Division Commander. The Administration Division Commander will assign personnel under the Administration Division Commander's command to administer the day-to-day operation of the ALPR equipment and data.

428.2.1 SPECIAL USE PERMITS

The Administration Division Commander or the authorized designee shall obtain required special use permits before installation of stationary ALPR equipment when applicable (Utah Code 41-6a-2003; Utah Code 72-1-212).

428.3 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. [Department/Office] personnel shall not use or allow others to use the equipment or database records for any unauthorized purpose.

- (a) An ALPR shall only be used for official and legitimate law enforcement business (Utah Code 41-6a-2003).
- (b) Particular consideration should be given to using ALPR-equipped vehicles to canvass areas around homicides, shootings, and other major incidents that qualify for use of an ALPR. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.
- (c) No member of this [department/office] shall operate ALPR equipment or access ALPR data without first completing [department/office]-approved training.
- (d) If practicable, the officer should verify an ALPR response through the appropriate law enforcement database before taking enforcement action that is based solely upon an ALPR alert.
- (e) No ALPR operator may access confidential [department/office], state, or federal data unless otherwise authorized to do so.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Automated License Plate Readers (ALPRs)

428.3.1 LIMITATIONS ON USE

ALPR data shall only be used for the following official law enforcement business (Utah Code 41-6a-2003):

- (a) As part of an active criminal investigation as defined by Utah Code 41-6a-2002
- (b) To apprehend an individual with an outstanding warrant
- (c) To locate a missing or endangered person
- (d) To locate a stolen vehicle

An ALPR system may be used to access the Utah Criminal Justice Information System to verify vehicle registration or insurance information, confirm vehicle identification, or identify a stolen vehicle (Utah Code 41-6a-2003).

428.4 DATA COLLECTION AND RETENTION

All data and images gathered by an ALPR are for the official use of the South Salt Lake Police Department and because such data may contain confidential information, it is not open to public review. ALPR information gathered and retained by this [department/office] may be used and shared with prosecutors or others only as permitted by law (Utah Code 41-6a-2004).

The Administration Division Commander is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with [department/office] procedures.

The Administration Division Commander or the authorized designee shall take steps to have all ALPR data that is not reasonably related to official law enforcement business purged in an unrecoverable manner as soon as practicable. In no event shall this data be maintained longer than nine months unless it is subject to a warrant, preservation request, or disclosure order (Utah Code 41-6a-2004). Data that will not be purged should be downloaded from the server onto portable media and booked into evidence.

428.4.1 NON-GOVERNMENTAL AGENCY ALPR

ALPR data captured by a non-governmental agency device may only be obtained pursuant to a warrant or a court order (Utah Code 41-6a-2005).

428.5 ACCOUNTABILITY

All data will be closely safeguarded and protected by both procedural and technological means. The South Salt Lake Police Department will observe the following safeguards regarding access to and use of stored data:

- (a) All ALPR data downloaded to the mobile workstation and server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.
- (b) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Automated License Plate Readers (ALPRs)

data relate to a specific criminal investigation or [department/office]-related civil or administrative action.

- (c) The number of ALPR data searches conducted by members as well as the crime type and incident numbers associated with each search shall be recorded and preserved for at least five years (Utah Code 41-6a-2005).
- (d) ALPR system audits should be conducted on a regular basis.

428.6 POLICY

The policy of the South Salt Lake Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this [department/office]. Because such data may contain confidential information, it is not open to public review.

428.7 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

- (a) The agency makes a written request for the ALPR data that includes:
 - 1. The name of the agency.
 - 2. The name of the person requesting.
 - 3. The intended purpose of obtaining the information.
- (b) The request is reviewed by the Administration Division Commander or the authorized designee and approved before the request is fulfilled.
- (c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.

428.8 PUBLIC ACCESS

This policy and any special use permits obtained for stationary ALPRs shall be published on the City website or on the Utah Public Notice Website if the [Department/Office] does not have access to a City website (Utah Code 41-6a-2003; Utah Code 72-1-212).

Unusual Occurrence and Planning and Review

429.1 TABLE OF CONTENTS

Unusual Occurrence Planning Functions included in this policy:

- Policy
- Mobile Incident Command Center
- Emergency Operations Plan Review
- Agency Mobilization Plan
- Stand-by Notification Procedures
- Agency Mobilization Plan Provisions
- Special Events Operations

429.1.1 POLICY

The South Salt Lake City Fire Department is responsible for overall emergency services planning for South Salt Lake City. The Fire Chief has appointed a team to develop and maintain the plan.

Within the police department, the Chief of Police or his/her designee is responsible for the maintenance of the law enforcement aspects of the plan, and to ensure that unusual occurrence planning unique to the police department, is developed and maintained.

429.1.2 MOBILE INCIDENT COMMAND CENTER (M.I.C.C.)

- (a) The following sections establish procedures for the deployment and maintenance of the South Salt Lake City Mobile Incident Command Center.
- (b) Definitions
 1. The Mobile Incident Command Center will be referred to as the M.I.C.C.
 2. M.I.C.C. Deployment Team refers to a group of trained individuals from police and fire that are trained in the deployment and operations of the M.I.C.C.
- (c) Maintenance and Care Procedures
 1. Regular maintenance and inspection of the M.I.C.C. will fall under the responsibility of the South Salt Lake City Fleet Department.
 2. Care and routine cleaning of the M.I.C.C. is a joint responsibility of the police and fire department. Assigned members from each department will be assigned to the M.I.C.C.
 3. Police and fire will ensure that the M.I.C.C. is cleaned and fueled after each deployment.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Unusual Occurrence and Planning and Review

4. Equipment repairs or alterations to the M.I.C.C. will be approved by the Chief of Police, Chief of Fire, or their designees.
- (d) Deployment
 1. Police Operations.
 2. Fire Operations.
 3. City Events.
 4. Any incident approved by the Mayor, Police Chief, Fire Chief or designees.
- (e) Deployment Authorization
 1. Police Operational Needs
 - (a) Deployment of the M.I.C.C. will be approved by a Commander or above.
 2. Fire Operational Needs
 - (a) Deployment of the M.I.C.C. will be approved by a Battalion Chief or above.
 3. The South Salt Lake City Mayor or designee may approve the deployment of the M.I.C.C. as needed.
- (f) M.I.C.C. Deployment Team
 - (a) Only trained members of the M.I.C.C. Team are authorized to mobilize the M.I.C.C. with authorized approval for deployment.
 - (b) All members of the M.I.C.C. Team will receive training in the operations, maneuvering, care and safety of the M.I.C.C.
 - (c) M.I.C.C. Team members will be on-call for after hour deployment. On-call compensation will be provided to each team member.
- (g) Operating Procedures
 - (a) M.I.C.C. Team members will wear a high visibility vest when operating in or around traffic.
 - (b) Team members will have knowledge of the overall height clearance of the M.I.C.C. and shall be familiar with all possible route obstructions prior to mobilization. Height familiarization of low hanging utility lines and bridges shall always be a priority. Under no circumstance should the M.I.C.C. be parked directly under a bridge or utility lines.
 - (c) Approved high visibility traffic cones will be placed at all four corners of the M.I.C.C. whenever stationary during a mobilization.
 - (d) Team members will chock a minimum of two (2) tires of the M.I.C.C. when in a stationary position during mobilization, or extended periods of parking.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Unusual Occurrence and Planning and Review

- (e) Team members will position the M.I.C.C. for curb side access whenever possible.
- (f) Team members should position the M.I.C.C. in a location of maximum visibility during mobilization. The M.I.C.C. should be easily recognized and located during incidents. The M.I.C.C. should not be placed in a position that would restrict the movement of additional apparatus to the scene.
- (g) Team members will not attempt to maneuver or back the M.I.C.C. without a minimum of two spotters. Spotters shall be placed at the right front of the vehicle and to the left rear of the vehicle whenever backing the M.I.C.C.
- (h) Confidentiality
 - (a) M.I.C.C. Team Members are prohibited from divulging information gleaned from any incident or deployment operations of the M.I.C.C.

429.1.3 EMERGENCY OPERATIONS PLAN REVIEW

The division commanders should review the effectiveness and viability of the current emergency operations plan, on an as-needed basis. Such a review may entail a mock situation occurrence, for purposes of evaluating, improving or updating the plans. Copies of the emergency operations plan are available to any department employee via the computer network and as designated by the Chief of Police.

429.1.4 AGENCY MOBILIZATION PLAN

- (a) Normally, an incident requiring the mobilization of all Department personnel, or a majority of them, can be planned ahead of time.
 - 1. If an incident or event is one for which plans have already been developed and have taken into account the provisions listed, the Department's mobilization plan may not need to be activated or implemented.
 - 2. However, there are some instances that happen spontaneously and escalate rapidly, or are massive and complex in nature, which may require the implementation of the Department's "Mobilization Plan".
- (b) If a situation or event occurs that immediately requires additional personnel to respond back to the City, the on-duty Sergeant or Watch Commander will contact the Division Commanders without delay to advise him/her of the situation.
 - 1. The Division Commanders will notify the Chief of Police or his/her designee as soon as practical.
 - 2. The Chief of Police will determine if notification of the Mayor and/or the other members on the City's Disaster Notification List is appropriate.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Unusual Occurrence and Planning and Review

- (c) If the Chief of Police orders the implementation of the mobilization plan, it will be accomplished systematically, and at the following alert stages:
 - 1. Level I:
 - (a) Level I consists of placing Department members on stand-by.
 - (b) The Division Commanders or his/her designee will notify all other appropriate personnel of the situation, and that they officially on "stand-by".
 - 1. The Division Commanders or his/her designee will notify personnel under his/her command of the "stand-by".
 - 2. The Department's mobilization plan will also address Communications:
 - (a) All participating officers will have access to communications, either by portable transceiver or mobile transceiver, or both.
 - (b) When personnel are place on "stand-by" they will be advised of the radio channel being used for the incident/event.
 - 2. Level II:
 - (a) Level II consists of certain members of the Department responding and staging.
 - 1. At this level, all Patrol Division personnel and the Division Commanders will be notified to respond to the station or designated staging area, as directed by the Chief of Police.
 - (b) The Chief of Police or his/her designee will:
 - 1. Oversee all Department activities.
 - 2. Assume command of all Department personnel.
 - 3. Assume command of the scene, pursuant to the provisions of the Memorandum of Understanding.
 - (c) The Division Commanders will:
 - 1. Brief personnel under his/her command of the situation.
 - 2. Ensure that personnel under his/her command are suitably and appropriately equipped and attired for the situation.
 - 3. Prepare to deploy his/her personnel as directed by the Chief of Police.
 - (d) The Division Commanders, unless otherwise directed by the Chief of Police, will assume command of the staging area.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Unusual Occurrence and Planning and Review

3. Level III

- (a) Level III consists of all other members of the Department being notified to respond to the staging area for briefing by the Division Commanders.

429.1.5 STANDBY NOTIFICATION PROCEDURES

- (a) When officers are placed on stand-by, they will be:

- 1. Called at home (if they are not on-duty). If no answer,
- 2. Called on their cellular phones. If no response,
- 3. VECC will be requested to try the officer on all radio channels.
- 4. If radio communications are inoperable, the incident commander or his/her designee will try to personally contact the officer.
- 5. All officers placed on "stand-by" will check their sources of communication (portable and mobile) immediately to ensure efficient operation.

- (b) Primary and Alternate Assembly Areas:

- 1. When officers are notified they are on "stand-by", they will also be advised of the primary staging area and any alternate staging area as well as the most appropriate and tactically sound way to approach the staging area.
- 2. Officers responding to the designated staging area will be advised of and provided with the anticipated equipment needed, by the respective Division Commander or his/her designee.
- 3. The creation and activation of special task forces to accomplish specific tasks or assignments will be done at the direction of the Chief of Police.

- (a) Personnel assigned to a task force will be deployed based upon criteria include, but not limited to:

- 1. The officer's level of expertise, education, and/or training in a given area.
- 2. Demonstrated proficiency with the equipment that the task force will utilize.
- 3. The availability of the officer.
- 4. Aside from the duties and responsibilities to be performed by the Chief of Police, Division Commanders, the Chief of Police will designate key personnel, with respect to such positions as a media liaison representative, and any other position the Chief of Police deems necessary.
- 5. Transportation - in the interest of time, the Chief of Police or Division Commander(s) or Patrol Watch Commander, may authorize personnel who are

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Unusual Occurrence and Planning and Review

already on-duty to pick-up employees who live near the City and who have been notified to respond to the staging area.

6. Management Control Measures - The Chief of Police or his/her designee will be responsible for all Department activities and personnel.
 - (a) Sergeants, Watch Commanders, Division Commanders, and the Chief of Police will be updated by those they supervise to ensure that tasks assigned have been performed.
 - (b) The Chief of Police will ensure that the City Mayor and/or other elected officials are notified, if necessary.
- (c) Rehearsals of the mobilization plan will be as directed by the Chief of Police or his/her designee.
 1. For authenticity, such rehearsals may involve Fire/Rescue, other City Offices, etc.

429.1.6 AGENCY MOBILIZATION PLAN PROVISIONS

- (a) The alert stages for the mobilization plan are identified in 463.1.4 above.
- (b) The procedures for notification of personnel during any emergency operation are identified in 463.1.5.
- (c) Primary and alternate assembly areas:
 1. The selection of an assembly area or incident command post will be the responsibility of the shift supervisor responding to the scene. Considerations should include:
 - (a) Adequate size, to include parking for multiple support units, shelter for evacuees, etc.
 - (b) Availability of telephone communications.
 - (c) Security considerations - is the area safe, but reasonable distance from the scene?
 1. The possibilities for incident command post sites include schools, churches, and office building.
 2. The size of the operation will dictate, in addition to the aforementioned tactical considerations, the size of an incident command post/assembly area.
- (d) Equipment specific to each emergency operation may be available, distributed, or already in the control of officers.
- (e) SWAT

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Unusual Occurrence and Planning and Review

1. The SWAT team will be pre-notified and should be called out on the following types of incidents, unless special circumstances dictate otherwise:
 - (a) Barricaded suspects.
 - (b) Hostage situations.
 - (c) High-risk search warrants.
 - (d) Other known high-risk situations.
 - (e) Other incidents deemed necessary by the Chief of Police.
2. The SWAT team will be subject to call-out regarding mutual aid requests made by outside agencies. The SWAT team call-out protocol is as follows:
 - (a) The SWAT Commander will approve all SWAT team call-outs.
 - (b) The SWAT Commander will brief the Chief of Police or his/her designee as soon as practical after approving the call-out.
 - (c) The incident commander will contact the tactical commander and/or the SWAT team leader.
 - (d) The incident commander may confer with the Chief of Police and/or his/her designee if necessary.
- (f) The SWAT team leader or designee will be responsible for mobilizing the tactical team members.
- (g) Additional Policies and Procedures governing the use of SWAT is contained in Chapter 4. Police 408, SWAT.
- (a) Key Personnel Designations - The highest-ranking officer/supervisor at an incident will be considered the incident commander until the arrival of the on-call commander, who may then take the position of incident commander.
 1. The incident commander will work closely with the hostage negotiator and/or SWAT team leader to coordinate a resolution to the incident.
 2. The incident commander will be responsible for the coordination of all other personnel, agencies, departments, etc. who may be called out to the incident.
 3. The number of officers involved as well as the anticipated number of evacuees, will generally dictate transportation requirements.
 - (a) While there is generally sufficient transportation available to handle our own units, it may be necessary to secure the use of the parks department's or public works' vehicles.
 - (b) Mass evacuations may involve school buses or public transportation.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Unusual Occurrence and Planning and Review

- (b) Management Control Measures - The designated "Civil Defense Liaison Officer" for South Salt Lake City is the South Salt Lake City Fire Chief.
 - (a) The Deputy Chief of Police will coordinate with the Fire Chief at least annually to evaluate and implement any modifications to the department civil disorder/disaster plan, to ensure that civil defense resources will be effectively utilized.
- (c) Rehearsals - The department may use an emergency operation incident rehearsal to educate employees on the proper procedures and protocol for major incidents.

429.1.7 SPECIAL EVENT OPERATIONS

- (a) The Division Commander, will at his/her discretion, designate a specific supervisor to oversee the handling and coordination of any special event.
 - 1. The supervisor will coordinate any requests of South Salt Lake City or outside agency assistance.
 - 2. The supervisor coordinating the event will provide the Division Commanders with:
 - (a) Written estimate of traffic, including a contingency plan for traffic diversion and control.
 - (b) Written estimate of crowd size and control plan.
 - (c) Written estimate of crime problems expected at any given event.
 - (d) Written list of logistical requirements.
 - 3. The supervisor will provide the Division Commanders with an estimate of the kind of resources needed to handle the event, including:
 - (a) The staffing needs, including any special operations personnel (sworn and non-sworn).
 - (b) All equipment needs (barricades, street cones, vehicles, etc.)
 - (c) All communication needs (between several agencies or departments, etc.)
 - (d) The need for centralized controls (command post other than the police department.)
 - (e) The estimated need for aid and medical services (to be coordinated with the fire department.)
 - (f) Liaison needs or problems (coordination with other departments or agencies.)
 - (g) A general deployment plan

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Unusual Occurrence and Planning and Review

4. The supervisor will be responsible for the operational supervision of such events when assigned and will generally be on-site to supervise those officers assigned for such events.
5. The Supervisor will be required to submit an after-event report to the affected Division Commander for debriefing and/or critique.

Homeless Persons

430.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure that personnel understand the needs and rights of the homeless and to establish procedures to guide officers during all contacts with the homeless, whether consensual or for enforcement purposes. The South Salt Lake Police Department recognizes that members of the homeless community are often in need of special protection and services. The South Salt Lake Police Department will address these needs in balance with the overall missions of this department. Therefore, officers will consider the following when serving the homeless community.

430.1.1 POLICY

It is the policy of the South Salt Lake Police Department to provide law enforcement services to all members of the community while protecting the rights, dignity and private property of the homeless. Homelessness is not a crime and members of this department will not use homelessness solely as a basis for detention or law enforcement action.

430.2 HOMELESS COMMUNITY LIAISON

The Chief of Police will designate a member of this department to act as the Homeless Liaison Officer. The responsibilities of the Homeless Liaison Officer include the following:

- (a) Maintain and make available to all department employees a list of assistance programs and other resources that are available to the homeless.
- (b) Meet with Social Services and representatives of other organizations that render assistance to the homeless.
- (c) Maintain a list of those areas within and near this jurisdiction that are used as frequent homeless encampments.
- (d) Remain abreast of laws dealing with the removal and/or destruction of the personal property of the homeless. This will include the following:
 - 1. Proper posting of notices of trespass and clean-up operations.
 - 2. Proper retention of property after clean-up, to include procedures for owners to reclaim their property in accordance with the Property and Evidence Policy and other established procedures.
- (e) Be present during any clean-up operation conducted by this department involving the removal of personal property of the homeless to ensure the rights of the homeless are not violated.
- (f) Develop training to assist officers in understanding current legal and social issues relating to the homeless.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Homeless Persons

430.3 FIELD CONTACTS

Officers are encouraged to contact the homeless for purposes of rendering aid, support and for community-oriented policing purposes. Nothing in this policy is meant to dissuade an officer from taking reasonable enforcement action when facts support a reasonable suspicion of criminal activity. However, when encountering a homeless person who has committed a non-violent misdemeanor and continued freedom is not likely to result in a continuation of the offense or a breach of the peace officers are encouraged to consider long-term solutions to problems that may relate to the homeless, such as shelter referrals and counseling in lieu of physical arrest.

Officers should provide homeless persons with resource and assistance information whenever it is reasonably apparent such services may be appropriate.

430.3.1 OTHER CONSIDERATIONS

Homeless members of the community will receive the same level and quality of service provided to other members of the community. The fact that a victim or witness is homeless can, however, require special considerations for a successful investigation and prosecution. Officers should consider the following when handling investigations involving homeless victims, witnesses or suspects:

- (a) Document alternate contact information. This may include obtaining addresses and phone numbers of relatives and friends.
- (b) Document places the homeless person may frequent.
- (c) Provide homeless victims with victim/witness resources when appropriate.
- (d) Obtain statements from all available witnesses in the event a homeless victim is unavailable for a court appearance.
- (e) Consider whether the person may be a dependent adult or elder and if so proceed in accordance with the Adult Abuse Policy.
- (f) Arrange for transportation for investigation related matters, such as medical exams and court appearances.
- (g) Consider whether a crime should be reported and submitted for prosecution even when a homeless victim indicates he/she does not desire prosecution.

430.4 PERSONAL PROPERTY

The personal property of homeless persons must not be treated differently than the property of other members of the public. Officers should use reasonable care when handling, collecting and retaining the personal property of homeless persons and should not destroy or discard the personal property of a homeless person.

When a homeless person is arrested, or otherwise removed from a public place, officers should make reasonable accommodations to permit the person to lawfully secure his/her personal property. Otherwise, the personal property should be collected for safekeeping. If the arrestee has more personal property than can reasonably be collected and transported by the officer, a

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Homeless Persons

supervisor should be consulted. The property should be photographed and measures should be taken to remove or secure the property. It will be the supervisor's responsibility to coordinate the removal and safekeeping of the property.

Officers should not conduct or assist in clean-up operations of belongings that reasonably appear to be the property of homeless persons without the prior authorization of a supervisor or the department Homeless Liaison Officer. When practicable, requests by the public for clean-up operations of a homeless encampment should be referred to the Homeless Liaison Officer.

Officers who encounter unattended encampments, bedding or other personal property in public areas that reasonably appears to belong to a homeless person should not remove or destroy such property and should inform the department Homeless Liaison Officer if such property appears to involve a trespass, blight to the community or is the subject of a complaint. It will be the responsibility of the Homeless Liaison Officer to address the matter in a timely fashion.

430.5 MENTAL ILLNESSES AND MENTAL IMPAIRMENTS

Some homeless persons may suffer from a mental illness or a mental impairment. Officers shall not detain a homeless person under a mental illness commitment unless facts and circumstances warrant such a detention (see the Civil Commitments Policy).

When a mental illness hold is not warranted, the contacting officer should provide the homeless person with contact information for mental health assistance as appropriate. In these circumstances, officers may provide transportation to a mental health specialist if requested by the person and approved by a supervisor.

430.6 ECOLOGICAL ISSUES

Sometimes homeless encampments can impact the ecology and natural resources of the community and may involve criminal offenses beyond mere littering. Officers are encouraged to notify other appropriate agencies or departments when a significant impact to the environment has or is likely to occur. Significant impacts to the environment may warrant a crime report, investigation, supporting photographs and supervisor notification.

Legal Process Service and Civil Standby's

431.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure sufficiency of information, accuracy, timeliness, accessibility, and fiscal responsibility in the delivery of legal process services not functional responsibility. Responsibilities shall be shared throughout the police department, and all affected Federal, State, and City criminal justice components.

431.1.1 LEGAL PROCESS SERVICE

- (a) Members of the South Salt Lake Police Department shall (when applicable) comply with the following guidelines:
 - 1. Records - Ensure that information regarding each item of legal process, civil and/or criminal, is recorded, and included the following elements:
 - (a) Date and Time Received.
 - (b) Type of legal Process, civil or criminal.
 - (c) Nature of Document.
 - (d) Source of document.
 - (e) Name of plaintiff/complaint or name of defendant/respondent.
 - (f) Officer assigned for service.
 - (g) Date of assignment.
 - (h) Court docket number.
 - (i) Date service is due.
 - 2. A record on the execution of attempted service of legal process documents is maintained and includes:
 - (a) Date and time service was executed/attempted.
 - (b) Name of Officer(s) executing/attempting service.
 - (c) Name of person on whom legal process was served/executed.
 - (d) Method of service/reason for non-service.
 - (e) Address of service/attempt.

431.1.2 SERVICE OF CIVIL PROCESS - PROTECTIVE ORDER SERVICE

The South Salt Lake City Police Department officers may serve Ex Parte Protective Orders and Non-expiring Protective Orders in emergency cases. The person being served must be named as a defendant in the order.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Legal Process Service and Civil Standby's

431.1.3 SERVICE OF CIVIL PROCESS - PROCEDURES

- (a) The officer may take the victim/plaintiff's service-stamped copy of the Ex Parte Protective Order, Summons and Complaint, or Non-Expiring Protective Order and serve it on the defendant, after identifying the defendant.
 - 1. The defendant must receive a copy of all documents, except the Proof of Service.
 - 2. Before giving the Ex Parte Protective Order, Summons and Complaint, or Non-expiring Protective Order to the defendant, the officer must complete the service-stamped information requested on the top right-hand corner of the document.
 - 3. The officer should also provide the requested service-stamped information on the copy left with the victim, along with one of his/her business cards.
 - (a) If the defendant violates the Order before the Salt Lake County Sheriff's Office or Third District Court receives the Proof of Service, the responding officer will be able to confirm that the Order has been served.
- (b) The officer must then complete a Proof of Service form, including the Court heading and case number, names of the defendant and plaintiff.
 - (a) The officer should mark the documents "served", and notify the VECC dispatcher of the service in order to alert any officers who may respond to the same location at a later time.
 - (b) The officer should retain a copy of the Ex Parte Protective Order, Summons and Complaint, or Non-expiring Protective Order, and the Proof of Service.
 - (c) The officer will then either FAX the information, or give the information and paperwork to his/her supervisor, to be routed to the day shift supervisor or the Records Department.
- (c) A copy of the Proof of Service form should be faxed as soon as possible to the Salt Lake County Sheriff's Office Civil Division at (801) 535-5805.
 - (a) A blank Proof of Service may have been attached to the copy of the Order for the officer's use.
- (d) A copy of the Order and Proof of Service will be held by the Records Department for verification of entry and storage.
 - (a) The original Proof of Service will then be sent to the Salt Lake County Sheriff's Office, Court Service Division, or as directed on documents.

431.1.4 CIVIL MATTERS - CIVIL STANDBY'S

The role of any police officer in a civil problem or dispute is a non-biased "Keep the Peace" posture. Any action on behalf of one party over the other needs to be at the direction of the court and after consulting the City or District Attorney's Office.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Legal Process Service and Civil Standby's

- (a) Officers are to "keep the peace", allowing both parties to resolve the issue. If that is not possible, both parties are to be separated. The possession of the property should remain status quo, and the parties advised to resolve the issue in the civil courts.
- (b) Seizure of property and property ownership is the ultimate responsibility of the Civil Courts.
- (c) Civil Court Orders or documents directed to any peace officer:
 - 1. It is easy to misunderstand these documents and their validity or status.
 - 2. It is our policy not to have officer's effect or serve process without direction from the City Attorney's Office.
 - 3. The primary responsibility for service of civil process is with the Salt Lake County Sheriff's Office or Constables Office pursuant to UCA 17-22-2.
- (d) Officers will follow all statutory and case law guidelines when executing criminal and civil processes.
- (e) Officers of this department should not execute civil process except as defined by law in specific limited areas, such as emergency protective orders.

431.1.5 CRIMINAL PROCESS - WARRANTS

- (a) South Salt Lake City Police Department officers may execute any criminal warrant (including the seizure of property) that is valid, but may only serve civil protective orders in emergency cases.
- (b) An officer may choose not to arrest at time of an incident, and have the City or District Attorney make a decision on having the court issue a summons, if charges are filed.
- (c) When serving warrants outside South Salt Lake City's Police jurisdiction, the officer should first notify the appropriate jurisdiction of intended action.
 - 1. If necessary, the officer should if needed request assistance from the appropriate agency, and in all cases, will notify them of anticipated difficulty.
- (d) The department will attempt to execute arrest warrants issued pursuant to traffic and criminal investigations conducted by the department and all other valid arrest warrants brought to its attention.

431.1.6 PROPERTY OBTAINED VIA LEGAL PROCESS

- (a) No property is obtained by this department, except by a valid search warrant process or by written permission by one having authority through the proper on-view seizure process, or other legally recognized procedure.
- (b) Items seized by search warrant are processed per current case law, department policy, and court rulings.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Legal Process Service and Civil Standby's

1. All property is to be listed by full description and serial numbers, if applicable.
 2. All monies are accounted for by denominations and, if necessary, serial numbers.
 - (a) The monies may be returned to the defendant, by receipt process if so ordered, or awarded to the city.
 3. All items are noted on department evidence forms and processed per policy.
- (c) Real property obtained by seizure may, after an appeal criterion is followed, be utilized or disposed of according to legal authority.

Removal of Patrons from Inn's or Motels

432.1 PURPOSE AND SCOPE

This policy is to address calls for service from innkeepers seeking to remove tenants who have breached their contract. While the law provides Rights to innkeepers, it does not provide a method for removing persons.

432.1.1 INN KEEPERS / MANAGER RESPONSIBILITIES

These incidents should be treated as civil matters until the officer determines:

1. The complainant is an employee of the establishment acting within the scope of his/her duties
2. There is a contract, or lack of dispute of fact regarding termination of tenancy
3. A good faith effort has been made by the complainant to resolve the matter civilly

432.1.2 POLICY

1. The officer engages in a Keep the Peace, ensuring no laws are broken as the innkeeper ejects the guest. If a guest or innkeeper escalates the situation into one involving assault or criminal mischief, the officer will take appropriate action. The officer should document the complaint and inform the guest of the innkeeper's right to eject him/her.
2. The officer will advise the tenant of his/her need to quit the premises or be subject to arrest for trespass. The officer may make a physical arrest; remove the tenant from the premises, then release on citation.
3. In determining a course of action an officer may consider factors, such as the age or health of the guest(s) to be ejected and if weather conditions will threaten the life or safety of the guest(s).

432.1.3 INNKEEPER'S RIGHTS -- LIABILITY -- PROHIBITION ON DISCRIMINATION.

U.C.A. 29-2-103.

(1) An innkeeper may:

(a) refuse or deny accommodations, facilities, or privileges of a lodging establishment to any person who is:

- (i) unwilling or unable to pay for the accommodations and services of the lodging establishment;
- (ii) visibly intoxicated;
- (iii) creating a public nuisance;
- (iv) in the reasonable belief of the innkeeper, seeking accommodations for any unlawful purpose, including:

- (A) the unlawful possession or use of controlled substances in violation of federal or state law; or
- (B) use of the premises for the consumption of alcoholic beverages by any person under 21 years of age in violation of federal or state law; or

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Removal of Patrons from Inn's or Motels

(v) in the reasonable belief of the innkeeper, bringing in property that may be dangerous to other persons, including firearms or explosives;

(b) require a prospective guest prior to check-in to demonstrate the guest's ability to pay either in cash, by credit card, or with a validated check;

(c) require a parent or legal guardian of a minor to:

(i) promise in writing to pay all guest room costs, taxes, and charges incurred by the minor at a lodging establishment and any damages to the lodging establishment and its furnishings caused by the minor while a guest at the lodging establishment;

(ii) provide an innkeeper with a valid credit card number to cover potential charges and any potential damages to the lodging establishment and its furnishings caused by the minor; or

(iii) if a valid credit card is not an option, provide an innkeeper with:

(A) an advance cash payment to cover the guest room costs and taxes for the anticipated stay of the minor; and

(B) a deposit, not to exceed \$500, towards the payment of any charges by the minor or any damages to the lodging establishment or its furnishings, which deposit shall be refunded to the extent not used to cover any damages as determined by the innkeeper following room inspection at check-out;

(d) require a guest to produce a valid driver's license, or other identification satisfactory to the innkeeper, containing a photograph and the name and address of the guest;

(e) if the guest is a minor, require a parent or guardian of the guest to register and produce the same identification required in Subsection (1)(d);

(f) limit the number of persons who may occupy a guest room in the lodging establishment;

(g) eject a person from a lodging establishment for any of the following reasons:

(i) nonpayment of the lodging establishment's charges for accommodations or services;

(ii) visible intoxication of the guest;

(iii) disorderly conduct of the guest resulting in a public nuisance; or

(iv) the innkeeper reasonably believes that the person has violated:

(A) this chapter or any federal, state, or local law or regulation relating to the lodging establishment; or

(B) any rule of the lodging establishment posted in a conspicuous place and manner in the lodging establishment.

(2) An innkeeper may not refuse or deny use of or eject a person from a lodging establishment's facilities or privileges based upon the person's race, creed, color, national origin, gender, disability, or marital status

Civil Disputes

433.1 PURPOSE AND SCOPE

This policy provides members of the South Salt Lake Police Department with guidance for addressing conflicts between persons when no criminal investigation or enforcement action is warranted (e.g., civil matters), with the goal of minimizing any potential for violence or criminal acts.

The Domestic Violence Policy will address specific legal mandates related to domestic violence court orders. References in this policy to “court orders” apply to any order of a court that does not require arrest or enforcement by the terms of the order or by Utah law.

433.2 POLICY

The South Salt Lake Police Department recognizes that a law enforcement presence at a civil dispute can play an important role in the peace and safety of the community. Subject to available resources, members of this [department/office] will assist at the scene of civil disputes with the primary goal of safeguarding persons and property, preventing criminal activity, and maintaining the peace. When handling civil disputes, members will remain impartial, maintain a calm presence, give consideration to all sides, and refrain from giving legal or inappropriate advice.

433.3 GENERAL CONSIDERATIONS

When appropriate, members handling a civil dispute should encourage the involved parties to seek the assistance of resolution services or take the matter to the civil courts. Members must not become personally involved in disputes and shall at all times remain impartial.

While not intended to be an exhaustive list, members should give considerations to the following when handling civil disputes:

- (a) Civil disputes tend to be confrontational and members should be alert that they can escalate to violence very quickly. De-escalation techniques should be used when appropriate.
- (b) Members should not dismiss alleged or observed criminal violations as a civil matter and should initiate the appropriate investigation and report when criminal activity is apparent.
- (c) Members shall not provide legal advice, however, when appropriate, members should inform the parties when they are at risk of violating criminal laws.
- (d) Members are reminded that they shall not enter a residence or other non-public location without legal authority including valid consent.
- (e) Members should not take an unreasonable amount of time assisting in these matters and generally should contact a supervisor if it appears that peacekeeping efforts longer than 30 minutes are warranted.

433.4 COURT ORDERS

Disputes involving court orders can be complex. Where no mandate exists for an officer to make an arrest for a violation of a court order, the matter should be addressed by documenting any apparent

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Civil Disputes

court order violation in a report. If there appears to be a more immediate need for enforcement action, the investigating officer should consult a supervisor prior to making any arrest.

If a person appears to be violating the terms of a court order but is disputing the validity of the order or its applicability, the investigating officer should document the following:

- (a) The person's knowledge of the court order or whether proof of service exists.
- (b) Any specific reason or rationale the involved person offers for not complying with the terms of the order.

A copy of the court order should be attached to the report when available. The report should be forwarded to the appropriate prosecutor. The report should also be forwarded to the court issuing the order with a notice that the report was also forwarded to the prosecutor for review.

433.4.1 STANDBY REQUESTS

Officers responding to a call for standby assistance to retrieve property should meet the person requesting assistance at a neutral location to discuss the process. The person should be advised that items that are disputed will not be allowed to be removed. The member may advise the person to seek private legal advice as to the distribution of disputed property.

Members should accompany the person to the location of the property. Members should ask if the other party will allow removal of the property or whether the other party would remove the property.

If the other party is uncooperative, the person requesting standby assistance should be instructed to seek private legal advice and obtain a court order to obtain the items. Officers should not order the other party to allow entry or the removal of any items. If there is a restraining or similar order against the person requesting standby assistance, that person should be asked to leave the scene or they may be subject to arrest for violation of the order.

If the other party is not present at the location, the member will not allow entry into the location or the removal of property from the location.

433.5 VEHICLES AND PERSONAL PROPERTY

Officers may be faced with disputes regarding possession or ownership of vehicles or other personal property. Officers may review documents provided by parties or available databases (e.g., vehicle registration), but should be aware that legal possession of vehicles or personal property can be complex. Generally, officers should not take any enforcement action unless a crime is apparent. The people and the vehicle or personal property involved should be identified and the incident documented.

433.6 REAL PROPERTY

Disputes over possession or occupancy of real property (e.g., land, homes, apartments) should generally be handled through a person seeking a court order.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Civil Disputes

433.6.1 LONG-TERM GUEST ISSUES

For disputes related to a long-term guest, as defined by Utah Code 76-6-206.4, who has received notice to vacate a residence by an owner, tenant, or other person with apparent authority to act for the owner or tenant, officers must provide the guest with a reasonable time to collect personal belongings prior to escorting the individual from the residence. A long-term guest should not be escorted from the residence if a separate owner or tenant has granted the guest express permission to remain in the residence and the permission has not been revoked or rendered void (Utah Code 76-6-206.4).

433.6.2 REMOVAL OF TRESPASSER FROM REAL PROPERTY

If a property owner or property owner's authorized agent requests the immediate removal of a trespasser from real property located within the jurisdiction of the South Salt Lake Police Department, the [department/office] will take reasonable steps to initiate action when appropriate in accordance with Utah Code 78B-6-817. If the trespasser is homeless or will be homeless following the removal, provisions of the Homeless Persons Policy should be followed to the extent practicable.

Public Recording of Law Enforcement Activity

434.1 PURPOSE AND SCOPE

This policy provides guidelines for handling situations in which members of the public photograph or audio/video record law enforcement actions and other public activities that involve members of this department. In addition, this policy provides guidelines for situations where the recordings may be evidence.

434.2 POLICY

The South Salt Lake Police Department recognizes the right of persons to lawfully record members of this department who are performing their official duties. Members of this department will not prohibit or intentionally interfere with such lawful recordings. Any recordings that are deemed to be evidence of a crime or relevant to an investigation will only be collected or seized lawfully.

Officers should exercise restraint and should not resort to highly discretionary arrests for offenses such as interference, failure to comply or disorderly conduct as a means of preventing someone from exercising the right to record members performing their official duties.

434.3 RECORDING LAW ENFORCEMENT ACTIVITY

Members of the public who wish to record law enforcement activities are limited only in certain aspects.

- (a) Recordings may be made from any public place or any private property where the individual has the legal right to be present.
- (b) Beyond the act of photographing or recording, individuals may not interfere with the law enforcement activity. Examples of interference include, but are not limited to:
 - 1. Tampering with a witness or suspect.
 - 2. Inciting others to violate the law.
 - 3. Being so close to the activity as to present a clear safety hazard to the officers.
 - 4. Being so close to the activity as to interfere with an officer's effective communication with a suspect or witness.
- (c) The individual may not present an undue safety risk to the officer, him/herself or others.
- (d) Recording the actions of an officer does not by itself constitute a crime of interference, willful resistance, disorderly conduct or obstruction of justice (Utah Code 76-8-305).

434.4 OFFICER RESPONSE

Officers should promptly request that a supervisor respond to the scene whenever it appears that anyone recording activities may be interfering with an investigation or it is believed that the recording may be evidence. If practicable, officers should wait for the supervisor to arrive before taking enforcement action or seizing any cameras or recording media.

Whenever practicable, officers or supervisors should give clear and concise warnings to individuals who are conducting themselves in a manner that would cause their recording or

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Public Recording of Law Enforcement Activity

behavior to be unlawful. Accompanying the warnings should be clear directions on what an individual can do to be compliant; directions should be specific enough to allow compliance. For example, rather than directing an individual to clear the area, an officer could advise the person that he/she may continue observing and recording from the sidewalk across the street.

If an arrest or other significant enforcement activity is taken as the result of a recording that interferes with law enforcement activity, officers shall document in a report the nature and extent of the interference or other unlawful behavior and the warnings that were issued.

434.5 SUPERVISOR RESPONSIBILITIES

A supervisor should respond to the scene when requested or any time the circumstances indicate a likelihood of interference or other unlawful behavior.

The supervisor should review the situation with the officer and:

- (a) Request any additional assistance as needed to ensure a safe environment.
- (b) Take a lead role in communicating with individuals who are observing or recording regarding any appropriate limitations on their location or behavior. When practical, the encounter should be recorded.
- (c) When practicable, allow adequate time for individuals to respond to requests for a change of location or behavior.
- (d) Ensure that any enforcement, seizure or other actions are consistent with this policy and constitutional and state law.
- (e) Explain alternatives for individuals who wish to express concern about the conduct of Department members, such as how and where to file a complaint.

434.6 SEIZING RECORDINGS AS EVIDENCE

Officers should not seize recording devices or media unless (42 USC § 2000aa):

- (a) There is probable cause to believe the person recording has committed or is committing a crime to which the recording relates, and the recording is reasonably necessary for prosecution of the person.
 - 1. Absent exigency or consent, a warrant should be sought before seizing or viewing such recordings. Reasonable steps may be taken to prevent erasure of the recording.
- (b) There is reason to believe that the immediate seizure of such recordings is necessary to prevent serious bodily injury or death of any person.
- (c) The person consents.
 - 1. To ensure that the consent is voluntary, the request should not be made in a threatening or coercive manner.
 - 2. If the original recording is provided, a copy of the recording should be provided to the recording party, if practicable. The recording party should be permitted to be present while the copy is being made, if feasible. Another way to obtain the

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Public Recording of Law Enforcement Activity

evidence is to transmit a copy of the recording from a device to a department-owned device.

Recording devices and media that are seized will be submitted within the guidelines of the Property and Evidence Policy.

Crisis Intervention Incidents

435.1 PURPOSE AND SCOPE

This policy provides guidelines for interacting with those who may be experiencing a mental health or emotional crisis. Interaction with such individuals has the potential for miscommunication and violence. It often requires an officer to make difficult judgments about a person's mental state and intent in order to effectively and legally interact with the individual.

435.1.1 DEFINITIONS

Definitions related to this policy include:

Person in crisis - A person whose level of distress or mental health symptoms have exceeded the person's internal ability to manage his/her behavior or emotions. A crisis can be precipitated by any number of things, including an increase in the symptoms of mental illness despite treatment compliance; non-compliance with treatment, including a failure to take prescribed medications appropriately; or any other circumstance or event that causes the person to engage in erratic, disruptive or dangerous behavior that may be accompanied by impaired judgment.

435.2 POLICY

The South Salt Lake Police Department is committed to providing a consistently high level of service to all members of the community and recognizes that persons in crisis may benefit from intervention. The Department will collaborate, where feasible, with mental health professionals to develop an overall intervention strategy to guide its members' interactions with those experiencing a mental health crisis. This is to ensure equitable and safe treatment of all involved.

435.3 SIGNS

Members should be alert to any of the following possible signs of mental health issues or crises:

- (a) A known history of mental illness
- (b) Threats of or attempted suicide
- (c) Loss of memory
- (d) Incoherence, disorientation or slow response
- (e) Delusions, hallucinations, perceptions unrelated to reality or grandiose ideas
- (f) Depression, pronounced feelings of hopelessness or uselessness, extreme sadness or guilt
- (g) Social withdrawal
- (h) Manic or impulsive behavior, extreme agitation, lack of control
- (i) Lack of fear
- (j) Anxiety, aggression, rigidity, inflexibility or paranoia

Members should be aware that this list is not exhaustive. The presence or absence of any of these should not be treated as proof of the presence or absence of a mental health issue or crisis.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Crisis Intervention Incidents

435.4 COORDINATION WITH MENTAL HEALTH PROFESSIONALS

The Chief of Police should designate an appropriate Division Commander to collaborate with mental health professionals to develop an education and response protocol. It should include a list of community resources, to guide department interaction with those who may be suffering from mental illness or who appear to be in a mental health crisis.

435.5 FIRST RESPONDERS

Safety is a priority for first responders. It is important to recognize that individuals under the influence of alcohol, drugs or both may exhibit symptoms that are similar to those of a person in a mental health crisis. These individuals may still present a serious threat to officers; such a threat should be addressed with reasonable tactics. Nothing in this policy shall be construed to limit an officer's authority to use reasonable force when interacting with a person in crisis.

Officers are reminded that mental health issues, mental health crises and unusual behavior alone are not criminal offenses. Individuals may benefit from treatment as opposed to incarceration.

An officer responding to a call involving a person in crisis should:

- (a) Promptly assess the situation independent of reported information and make a preliminary determination regarding whether a mental health crisis may be a factor.
- (b) Request available backup officers and specialized resources as deemed necessary and, if it is reasonably believed that the person is in a crisis situation, use conflict resolution and de-escalation techniques to stabilize the incident as appropriate.
- (c) If feasible, and without compromising safety, turn off flashing lights, bright lights or sirens.
- (d) Attempt to determine if weapons are present or available.
- (e) Take into account the person's mental and emotional state and potential inability to understand commands or to appreciate the consequences of his/her action or inaction, as perceived by the officer.
- (f) Secure the scene and clear the immediate area as necessary.
- (g) Employ tactics to preserve the safety of all participants.
- (h) Determine the nature of any crime.
- (i) Request a supervisor, as warranted.
- (j) Evaluate any available information that might assist in determining cause or motivation for the person's actions or stated intentions.
- (k) If circumstances reasonably permit, consider and employ alternatives to force.

435.6 DE-ESCALATION

Officers should consider that taking no action or passively monitoring the situation may be the most reasonable response to a mental health crisis.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Crisis Intervention Incidents

Once it is determined that a situation is a mental health crisis and immediate safety concerns have been addressed, responding members should be aware of the following considerations and should generally:

- Evaluate safety conditions.
- Introduce themselves and attempt to obtain the person's name.
- Be patient, polite, calm, courteous and avoid overreacting.
- Speak and move slowly and in a non-threatening manner.
- Moderate the level of direct eye contact.
- Remove distractions or disruptive people from the area.
- Demonstrate active listening skills (e.g., summarize the person's verbal communication).
- Provide for sufficient avenues of retreat or escape should the situation become volatile.

Responding officers generally should not:

- Use stances or tactics that can be interpreted as aggressive.
- Allow others to interrupt or engage the person.
- Corner a person who is not believed to be armed, violent or suicidal.
- Argue, speak with a raised voice or use threats to obtain compliance.

435.7 INCIDENT ORIENTATION

When responding to an incident that may involve mental illness or a mental health crisis, the officer should request that the dispatcher provide critical information as it becomes available. This includes:

- (a) Whether the person relies on drugs or medication, or may have failed to take his/her medication.
- (b) Whether there have been prior incidents, suicide threats/attempts, and whether there has been previous police response.
- (c) Contact information for a treating physician or mental health professional.

Additional resources and a supervisor should be requested as warranted.

435.8 SUPERVISOR RESPONSIBILITIES

A supervisor should respond to the scene of any interaction with a person in crisis. Responding supervisors should:

- (a) Attempt to secure appropriate and sufficient resources.
- (b) Closely monitor any use of force, including the use of restraints, and ensure that those subjected to the use of force are provided with timely access to medical care (see the Handcuffing and Restraints Policy).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Crisis Intervention Incidents

- (c) Consider strategic disengagement. Absent an imminent threat to the public and, as circumstances dictate, this may include removing or reducing law enforcement resources or engaging in passive monitoring.
- (d) Ensure that all reports are completed and that incident documentation uses appropriate terminology and language.
- (e) Conduct an after-action tactical and operational debriefing, and prepare an after-action evaluation of the incident to be forwarded to the Division Commander.
- (f) Evaluate whether a critical incident stress management debriefing for involved members is warranted.

435.9 INCIDENT REPORTING

Members engaging in any oral or written communication associated with a mental health crisis should be mindful of the sensitive nature of such communications and should exercise appropriate discretion when referring to or describing persons and circumstances.

Members having contact with a person in crisis should keep related information confidential, except to the extent that revealing information is necessary to conform to department reporting procedures or other official mental health or medical proceedings.

435.9.1 DIVERSION

Individuals who are not being arrested should be processed in accordance with the Civil Commitments Policy.

435.10 NON-SWORN INTERACTION WITH PEOPLE IN CRISIS

Non-sworn members may be required to interact with persons in crisis in an administrative capacity, such as dispatching, records request, and animal control issues.

- (a) Members should treat all individuals equally and with dignity and respect.
- (b) If a member believes that he/she is interacting with a person in crisis, he/she should proceed patiently and in a calm manner.
- (c) Members should be aware and understand that the person may make unusual or bizarre claims or requests.

If a person's behavior makes the member feel unsafe, if the person is or becomes disruptive or violent, or if the person acts in such a manner as to cause the member to believe that the person may be harmful to him/herself or others, an officer should be promptly summoned to provide assistance.

435.11 EVALUATION

The Division Commander designated to coordinate the crisis intervention strategy for this department should ensure that a thorough review and analysis of the department response to these incidents is conducted annually. The report will not include identifying information pertaining to any involved individuals, officers or incidents and will be submitted to the Chief of Police through the chain of command.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Crisis Intervention Incidents

435.12 TRAINING

In coordination with the mental health community and appropriate stakeholders, the Department will develop and provide comprehensive education and training to all department members to enable them to effectively interact with persons in crisis.

Medical Aid and Response

436.1 PURPOSE AND SCOPE

This policy recognizes that members often encounter persons in need of medical aid and establishes a law enforcement response to such situations.

436.2 POLICY

It is the policy of the South Salt Lake Police Department that all officers and other designated members be trained to provide emergency medical aid and to facilitate an emergency medical response.

436.3 FIRST RESPONDING MEMBER RESPONSIBILITIES

Whenever practicable, members should take appropriate steps to provide initial medical aid (e.g., first aid, CPR, use of an automated external defibrillator (AED)) in accordance with their training and current certification levels. This should be done for those in need of immediate care and only when the member can safely do so.

Prior to initiating medical aid, the member should contact Dispatch and request response by Emergency Medical Services (EMS) as the member deems appropriate.

Members should follow universal precautions when providing medical aid, such as wearing gloves and avoiding contact with bodily fluids, consistent with the Communicable Diseases Policy. Members should use a barrier or bag device to perform rescue breathing.

When requesting EMS, the member should provide Dispatch with information for relay to EMS personnel in order to enable an appropriate response, including:

- (a) The location where EMS is needed.
- (b) The nature of the incident.
- (c) Any known scene hazards.
- (d) Information on the person in need of EMS, such as:
 - 1. Signs and symptoms as observed by the member.
 - 2. Changes in apparent condition.
 - 3. Number of patients, sex, and age, if known.
 - 4. Whether the person is conscious, breathing, and alert, or is believed to have consumed drugs or alcohol.
 - 5. Whether the person is showing signs of extreme agitation or is engaging in violent irrational behavior accompanied by profuse sweating, extraordinary strength beyond their physical characteristics, and imperviousness to pain.

Members should stabilize the scene whenever practicable while awaiting the arrival of EMS.

Members should not direct EMS personnel whether to transport the person for treatment.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Medical Aid and Response

436.4 TRANSPORTING ILL AND INJURED PERSONS

Except in exceptional cases where alternatives are not reasonably available, members should not transport persons who are not in custody and who are unconscious, who have serious injuries, or who may be seriously ill. EMS personnel should be called to handle patient transportation.

For guidelines regarding transporting ill or injured persons who are in custody, see the Transporting Persons in Custody Policy.

Members should not provide emergency escort for medical transport or civilian vehicles.

436.5 PERSONS REFUSING EMS CARE

If a person who is not in custody refuses EMS care or refuses to be transported to a medical facility, an officer shall not force that person to receive care or be transported. However, members may assist EMS personnel when EMS personnel determine the person lacks mental capacity to understand the consequences of refusing medical care or to make an informed decision and the lack of immediate medical attention may result in serious bodily injury or the death of the person.

In cases where mental illness may be a factor, the officer should consider proceeding with temporary custody pursuant to a civil commitment in accordance with the Civil Commitments Policy.

If an officer believes that a person who is in custody requires EMS care and the person refuses, he/she should encourage the person to receive medical treatment. The officer may also consider contacting a family member to help persuade the person to agree to treatment or who may be able to authorize treatment for the person.

If the person who is in custody still refuses, the officer will require the person to be transported to the nearest medical facility. In such cases, the officer should consult with a supervisor prior to the transport.

Members shall not sign refusal-for-treatment forms or forms accepting financial responsibility for treatment.

436.6 SICK OR INJURED ARRESTEE

If an arrestee appears ill or injured, or claims illness or injury, the arrestee should be medically cleared prior to booking. If the officer has reason to believe the arrestee is feigning injury or illness, the officer should contact a supervisor, who will determine whether medical clearance will be obtained prior to booking.

If the jail or detention facility refuses to accept custody of an arrestee based on medical screening, the officer should note the name of the facility person refusing to accept custody and the reason for refusal, and should notify a supervisor to determine the appropriate action.

Arrestees who appear to have a serious medical issue should be transported by ambulance to an appropriate medical facility.

Nothing in this section should delay an officer from requesting EMS when an arrestee reasonably appears to be exhibiting symptoms that appear to be life threatening, including breathing problems

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Medical Aid and Response

or an altered level of consciousness, or is claiming an illness or injury that reasonably warrants an EMS response in accordance with the officer's training.

436.6.1 HOSPITAL SECURITY AND CONTROL

Officers who transport persons in custody to medical facilities for treatment should provide security and control during examination and treatment consistent with [department/office] protocols. Any such transport should be conducted in accordance with the Transporting Persons in Custody Policy.

The Patrol Division Commander should develop protocols related to the following:

- (a) Providing security and control during an examination or treatment, including:
 1. Monitoring the person in custody (e.g., guarding against escape, suicide, and assault of others)
 2. Removal of restraints, if necessary and appropriate (see the Handcuffing and Restraints Policy)
- (b) Responsibility for continuing security and control if the person in custody is admitted to the hospital
 1. This should include transferring custody of the person to an appropriate agency.

436.7 MEDICAL ATTENTION RELATED TO USE OF FORCE

Specific guidelines for medical attention for injuries sustained from a use of force may be found in the Use of Force, Handcuffing and Restraints, Control Devices and Techniques, and Conducted Energy Device policies.

436.8 AIR AMBULANCE

Generally, when on-scene, EMS personnel will be responsible for determining whether an air ambulance response should be requested. An air ambulance may be appropriate when there are victims with life-threatening injuries or who require specialized treatment (e.g., gunshot wounds, burns, obstetrical cases), and distance or other known delays will affect the EMS response.

The Patrol Division Commander should develop guidelines for air ambulance landings or enter into local operating agreements for the use of air ambulances, as applicable. In creating those guidelines, the Department should identify:

- Responsibility and authority for designating a landing zone and determining the size of the landing zone.
- Responsibility for securing the area and maintaining that security once the landing zone is identified.
- Consideration of the air ambulance provider's minimum standards for proximity to vertical obstructions and surface composition (e.g., dirt, gravel, pavement, concrete, grass).
- Consideration of the air ambulance provider's minimum standards for horizontal clearance from structures, fences, power poles, antennas or roadways.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Medical Aid and Response

- Responsibility for notifying the appropriate highway or transportation agencies if a roadway is selected as a landing zone.
- Procedures for ground personnel to communicate with flight personnel during the operation.

One department member at the scene should be designated as the air ambulance communications contact. Headlights, spotlights and flashlights should not be aimed upward at the air ambulance. Members should direct vehicle and pedestrian traffic away from the landing zone.

Members should follow these cautions when near an air ambulance:

- Never approach the aircraft until signaled by the flight crew.
- Always approach the aircraft from the front.
- Avoid the aircraft's tail rotor area.
- Wear eye protection during landing and take-off.
- Do not carry or hold items, such as IV bags, above the head.
- Ensure that no one smokes near the aircraft.

436.9 AUTOMATED EXTERNAL DEFIBRILLATOR (AED) USE

A member should use an AED only after the member has received appropriate training (Utah Code 53-2d-806).

436.9.1 AED USER RESPONSIBILITY

Members who are issued AEDs should check the AED at the beginning of the shift to ensure it is properly charged and functioning. Any AED that is not functioning properly shall be taken out of service and given to the Training Coordinator who is responsible for ensuring appropriate maintenance.

Following use of an AED, the device shall be cleaned and/or decontaminated as required. The electrodes and/or pads will be replaced as recommended by the AED manufacturer.

Any member who uses an AED should contact Dispatch as soon as possible and request response by EMS.

436.9.2 AED REPORTING

Any member using an AED will complete an incident report detailing its use.

436.9.3 AED TRAINING AND MAINTENANCE

The Training Coordinator should ensure appropriate training, that includes training in CPR and AED use, is provided to members authorized to use an AED (Utah Code 53-2d-806).

The Training Coordinator is responsible for ensuring AED devices are appropriately maintained and will retain records of all maintenance in accordance with the established records retention schedule.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Medical Aid and Response

436.10 ADMINISTRATION OF OPIOID OVERDOSE MEDICATION

Members may administer opioid overdose medication in accordance with protocol specified by the health care provider who prescribed the overdose medication for use by the member. With approval of the on-duty supervisor, members may also provide the opioid overdose medication to a person who is experiencing an opiate-related drug overdose event or to a family member, friend, or other individual who is in a position to assist such individual (Utah Code 26B-4-509).

436.10.1 OPIOID OVERDOSE MEDICATION USER RESPONSIBILITIES

Members who are qualified to administer opioid overdose medication, such as naloxone, should handle, store and administer the medication consistent with their training. Members should check the medication and associated administration equipment at the beginning of their shift to ensure they are serviceable and not expired. Any expired medication or unserviceable administration equipment should be removed from service and given to the Training Coordinator.

Any member who administers an opioid overdose medication should contact Dispatch as soon as possible and request response by EMS.

436.10.2 OPIOID OVERDOSE MEDICATION REPORTING

Any member administering opioid overdose medication should detail its use in an appropriate report.

The Training Coordinator will ensure that the Records Supervisor is provided enough information to meet applicable state reporting requirements.

436.10.3 OPIOID OVERDOSE MEDICATION TRAINING

The Training Coordinator should ensure training is provided to members authorized to administer opioid overdose medication. The training should include the written instructions provided by the dispensing health care provider on (Utah Code 26B-4-509):

- (a) How to recognize an opiate-related drug overdose event.
- (b) How to administer an opiate antagonist.
- (c) How to ensure that an individual to whom the medication has been administered receives additional medical care and a medical evaluation, as soon as possible.

436.11 FIRST-AID TRAINING

The Training Coordinator should ensure officers receive periodic first-aid training appropriate for their position.

First Amendment Assemblies

437.1 PURPOSE AND SCOPE

This policy provides guidance for responding to public assemblies or demonstrations.

437.2 POLICY

The South Salt Lake Police Department respects the rights of people to peaceably assemble. It is the policy of this department not to unreasonably interfere with, harass, intimidate or discriminate against persons engaged in the lawful exercise of their rights, while also preserving the peace, protecting life and preventing the destruction of property.

437.3 GENERAL CONSIDERATIONS

Individuals or groups present on the public way, such as public facilities, streets or walkways, generally have the right to assemble, rally, demonstrate, protest or otherwise express their views and opinions through varying forms of communication, including the distribution of printed matter. These rights may be limited by laws or ordinances regulating such matters as the obstruction of individual or vehicle access or egress, trespass, noise, picketing, distribution of handbills and leafleting, and loitering. However, officers shall not take action or fail to take action based on the opinions being expressed.

Participant behavior during a demonstration or other public assembly can vary. This may include, but is not limited to:

- Lawful, constitutionally protected actions and speech.
- Civil disobedience (typically involving minor criminal acts).
- Rioting.

All of these behaviors may be present during the same event. Therefore, it is imperative that law enforcement actions are measured and appropriate for the behaviors officers may encounter. This is particularly critical if force is being used. Adaptable strategies and tactics are essential. The purpose of a law enforcement presence at the scene of public assemblies and demonstrations should be to preserve the peace, to protect life and prevent the destruction of property.

Officers should not:

- (a) Engage in assembly or demonstration-related discussion with participants.
- (b) Harass, confront or intimidate participants.
- (c) Seize the cameras, cell phones or materials of participants or observers unless an officer is placing a person under lawful arrest.

Supervisors should continually observe department members under their commands to ensure that members' interaction with participants and their response to crowd dynamics is appropriate.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

First Amendment Assemblies

437.3.1 PHOTOGRAPHS AND VIDEO RECORDINGS

Photographs and video recording, when appropriate, can serve a number of purposes, including support of criminal prosecutions by documenting criminal acts; assistance in evaluating department performance; serving as training material; recording the use of dispersal orders; and facilitating a response to allegations of improper law enforcement conduct.

Photographs and videos will not be used or retained for the sole purpose of collecting or maintaining information about the political, religious or social views of associations, or the activities of any individual, group, association, organization, corporation, business or partnership, unless such information directly relates to an investigation of criminal activities and there is reasonable suspicion that the subject of the information is involved in criminal conduct.

437.4 UNPLANNED EVENTS

When responding to an unplanned or spontaneous public gathering, the first responding officer should conduct an assessment of conditions, including, but not limited to, the following:

- Location
- Number of participants
- Apparent purpose of the event
- Leadership (whether it is apparent and/or whether it is effective)
- Any initial indicators of unlawful or disruptive activity
- Indicators that lawful use of public facilities, streets or walkways will be impacted
- Ability and/or need to continue monitoring the incident

Initial assessment information should be promptly communicated to Dispatch, and the assignment of a supervisor should be requested. Additional resources should be requested as appropriate. The responding supervisor shall assume command of the incident until command is expressly assumed by another, and the assumption of command is communicated to the involved members. A clearly defined command structure that is consistent with the Incident Command System (ICS) should be established as resources are deployed.

437.4.1 CRIMINAL STREET GANGS

Officers should conduct gang-loitering enforcement in a manner consistent with Utah law and should not infringe on the right of individuals to engage in constitutionally protected collective advocacy activities (e.g., lawful picketing, demonstrations, religious or political assembly) (Utah Code 53-25-602).

437.5 PLANNED EVENT PREPARATION

For planned events, comprehensive, incident-specific operational plans should be developed. The ICS should be considered for such events.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

First Amendment Assemblies

437.5.1 INFORMATION GATHERING AND ASSESSMENT

In order to properly assess the potential impact of a public assembly or demonstration on public safety and order, relevant information should be collected and vetted. This may include:

- Information obtained from outreach to group organizers or leaders.
- Information about past and potential unlawful conduct associated with the event or similar events.
- The potential time, duration, scope, and type of planned activities.
- Any other information related to the goal of providing a balanced response to criminal activity and the protection of public safety interests.

Information should be obtained in a transparent manner, and the sources documented. Relevant information should be communicated to the appropriate parties in a timely manner.

Information will be obtained in a lawful manner and will not be based solely on the purpose or content of the assembly or demonstration, or actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability of the participants (or any other characteristic that is unrelated to criminal conduct or the identification of a criminal subject).

437.5.2 OPERATIONAL PLANS

An operational planning team with responsibility for event planning and management should be established. The planning team should develop an operational plan for the event.

The operational plan will minimally provide for:

- (a) Command assignments, chain of command structure, roles and responsibilities.
- (b) Staffing and resource allocation.
- (c) Management of criminal investigations.
- (d) Designation of uniform of the day and related safety equipment (e.g., helmets, shields).
- (e) Deployment of specialized resources.
- (f) Event communications and interoperability in a multijurisdictional event.
- (g) Liaison with demonstration leaders and external agencies.
- (h) Liaison with City government and legal staff.
- (i) Media relations.
- (j) Logistics: food, fuel, replacement equipment, duty hours, relief and transportation.
- (k) Traffic management plans.
- (l) First aid and emergency medical service provider availability.
- (m) Prisoner transport and detention.
- (n) Review of policies regarding public assemblies and use of force in crowd control.
- (o) Parameters for declaring an unlawful assembly.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

First Amendment Assemblies

- (p) Arrest protocol, including management of mass arrests.
- (q) Protocol for recording information flow and decisions.
- (r) Rules of engagement, including rules of conduct, protocols for field force extraction and arrests, and any authorization required for the use of force.
- (s) Protocol for handling complaints during the event.
- (t) Parameters for the use of body-worn cameras and other portable recording devices.

437.5.3 MUTUAL AID AND EXTERNAL RESOURCES

The magnitude and anticipated duration of an event may necessitate interagency cooperation and coordination. The assigned Incident Commander should ensure that any required memorandums of understanding or other agreements are properly executed, and that any anticipated mutual aid is requested and facilitated (see the Outside Agency Assistance Policy).

437.6 UNLAWFUL ASSEMBLY DISPERSAL ORDERS

If a public gathering or demonstration remains peaceful and nonviolent, and there is no reasonably imminent threat to persons or property, the Incident Commander should generally authorize continued monitoring of the event.

Should the Incident Commander make a determination that public safety is presently or is about to be jeopardized, the Incident Commander or the authorized designee should attempt to verbally persuade event organizers or participants to disperse of their own accord. Warnings and advisements may be communicated through established communications links with leaders and/or participants or to the group.

When initial attempts at verbal persuasion are unsuccessful, the Incident Commander or the authorized designee should make a clear standardized announcement to the gathering that the event is an unlawful assembly, and should order the dispersal of the participants. The announcement should be communicated by whatever methods are reasonably available to ensure that the content of the message is clear and that it has been heard by the participants. The announcement should be amplified, made in different languages as appropriate, made from multiple locations in the affected area, and documented by audio and video. The announcement should provide information about what law enforcement actions will take place if illegal behavior continues and should identify routes for egress. A reasonable time to disperse should be allowed following a dispersal order.

437.7 USE OF FORCE

Use of force is governed by current [department/office] policy and applicable law (see the Use of Force, Handcuffing and Restraints, Control Devices and Techniques, and Conducted Energy Device policies).

Individuals refusing to comply with lawful orders (e.g., nonviolent refusal to disperse) should be given a clear verbal warning and a reasonable opportunity to comply. If an individual refuses to comply with lawful orders, the Incident Commander shall evaluate the type of resistance and adopt

South Salt Lake Police Department

South Salt Lake PD Policy Manual

First Amendment Assemblies

a reasonable response in order to accomplish the law enforcement mission (such as dispersal or arrest of those acting in violation of the law). Control devices and conducted energy devices should be considered only when the participants' conduct reasonably appears to present the potential to harm officers, themselves or others, or will result in substantial property loss or damage (see the Control Devices and Techniques and the Conducted Energy Device policies).

Force or control devices, including oleoresin capsaicin (OC), should be directed toward individuals and not toward groups or crowds, unless specific individuals cannot reasonably be targeted due to extreme circumstances, such as a riotous crowd.

Any use of force by a member of this [department/office] shall be documented promptly, completely, and accurately in an appropriate report. The type of report required may depend on the nature of the incident.

437.8 ARRESTS

The South Salt Lake Police Department should respond to unlawful behavior in a manner that is consistent with the operational plan. If practicable, warnings or advisements should be communicated prior to arrest.

Mass arrests should be employed only when alternate tactics and strategies have been, or reasonably appear likely to be, unsuccessful. Mass arrests shall only be undertaken upon the order of the Incident Commander or the authorized designee. There must be probable cause for each arrest.

If employed, mass arrest protocols should fully integrate:

- (a) Reasonable measures to address the safety of officers and arrestees.
- (b) Dedicated arrest, booking and report writing teams.
- (c) Timely access to medical care.
- (d) Timely access to legal resources.
- (e) Timely processing of arrestees.
- (f) Full accountability for arrestees and evidence.
- (g) Coordination and cooperation with the prosecuting authority, jail and courts (see the Citation Releases Policy).

437.9 MEDIA RELATIONS

The Public Information Officer should use all available avenues of communication, including press releases, briefings, press conferences and social media to maintain open channels of communication with media representatives and the public about the status and progress of the event, taking all opportunities to reassure the public about the professional management of the event (see the Media Relations Policy).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

First Amendment Assemblies

437.10 DEMOBILIZATION

When appropriate, the Incident Commander or the authorized designee should implement a phased and orderly withdrawal of law enforcement resources. All relieved personnel should promptly complete any required reports, including use of force reports, and account for all issued equipment and vehicles to their supervisors prior to returning to normal operational duties.

437.11 POST EVENT

The Incident Commander should designate a member to assemble full documentation of the event, to include the following:

- (a) Operational plan
- (b) Any incident logs
- (c) Any assignment logs
- (d) Vehicle, fuel, equipment and supply records
- (e) Incident, arrest, use of force, injury and property damage reports
- (f) Photographs, audio/video recordings, Dispatch records/tapes
- (g) Media accounts (print and broadcast media)

437.11.1 AFTER-ACTION REPORTING

The Incident Commander should work with City legal counsel, as appropriate, to prepare a comprehensive after-action report of the event, explaining all incidents where force was used including the following:

- (a) Date, time and description of the event
- (b) Actions taken and outcomes (e.g., injuries, property damage, arrests)
- (c) Problems identified
- (d) Significant events
- (e) Recommendations for improvement; opportunities for training should be documented in a generic manner, without identifying individuals or specific incidents, facts or circumstances.

437.12 TRAINING

Department members should receive periodic training regarding this policy, as well as the dynamics of crowd control and incident management. The Department should, when practicable, train with its external and mutual aid partners.

Suspicious Activity Reporting

438.1 PURPOSE AND SCOPE

This policy provides guidelines for reporting and investigating suspicious and criminal activity.

438.1.1 DEFINITIONS

Definitions related to this policy include:

Involved party - An individual who has been observed engaging in suspicious activity, as defined in this policy, when no definitive criminal activity can be identified, thus precluding the person's identification as a suspect.

Suspicious activity - Any reported or observed activity that a member reasonably believes may have a nexus to any criminal act or attempted criminal act, or to foreign or domestic terrorism. Actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability should not be considered as factors that create suspicion (although these factors may be used as specific suspect descriptions). Examples of suspicious activity may include but are not limited to:

- Suspected pre-operational surveillance or intelligence gathering (e.g., photographing security features, asking questions about sensitive security-related subjects).
- Tests of security measures and response to incidents (e.g., "dry run," creating false alarms, attempts to enter secure areas without authorization).
- Suspicious purchases (e.g., purchasing large quantities of otherwise legal items, such as fertilizer, that could be used to create an explosive or other dangerous device).
- An individual in possession of such things as a hoax explosive or dispersal device, sensitive materials (e.g., passwords, access codes, classified government information), or coded or ciphered literature or correspondence.

Suspicious Activity Report (SAR) - An incident report used to document suspicious activity.

438.2 POLICY

The South Salt Lake Police Department recognizes the need to protect the public from criminal conduct and acts of terrorism and shall lawfully collect, maintain and disseminate information regarding suspicious activities, while safeguarding civil liberties and privacy protections.

438.3 RESPONSIBILITIES

The Investigation Division Commander and authorized designees will manage SAR activities. Authorized designees should include supervisors who are responsible for department participation in criminal intelligence systems as outlined in the Criminal Organizations Policy.

The responsibilities of the Investigation Division Commander include, but are not limited to:

- (a) Remaining familiar with those databases available to the Department that would facilitate the purpose of this policy.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Suspicious Activity Reporting

- (b) Maintaining adequate training in the area of intelligence gathering to ensure no information is being maintained that would violate the law or civil rights of any individual.
- (c) Ensuring a process is available that would allow members to report relevant information. The process should be designed to promote efficient and quick reporting, and should not be cumbersome, duplicative or complicated.
- (d) Ensuring that members are made aware of the purpose and value of documenting information regarding suspicious activity, as well as the databases and other information resources that are available to the Department.
- (e) Ensuring that SAR information is appropriately disseminated to members in accordance with their job responsibilities.
- (f) Coordinating investigative follow-up, if appropriate.
- (g) Coordinating with any appropriate agency or fusion center.
- (h) Ensuring that, as resources are available, the Department conducts outreach that is designed to encourage members of the community to report suspicious activity and that outlines what they should look for and how they should report it (e.g., website, public service announcements).

438.4 REPORTING AND INVESTIGATION

Any department member receiving information regarding suspicious activity should take any necessary immediate and appropriate action, including a request for tactical response or immediate notification of specialized entities, when applicable. Any non-sworn member who receives such information should ensure that it is passed on to an officer in a timely manner.

If the suspicious activity is not directly related to a reportable crime, the member should prepare a SAR and include information about involved parties and the circumstances of the incident. If, during any investigation, an officer becomes aware of suspicious activity that is unrelated to the current investigation, the information should be documented separately in a SAR and not included in the original incident report. The report number of the original incident should be included in the SAR as a cross reference. A SAR should be processed as any other incident report.

438.5 HANDLING INFORMATION

The Records Section will forward copies of SARs, in a timely manner, to the following:

- Investigations Division supervisor
- Crime Analysis Unit
- Other authorized designees

School Resource Officers

439.1 PURPOSE AND SCOPE

This policy describes the South Salt Lake Police Department School Resource Officer (SRO) program (Utah Code 53-10-117).

439.2 POLICY

The South Salt Lake Police Department is committed to enhancing the safety of students and faculty on campuses located in the [department/office]'s jurisdiction by forming a partnership with school administrators, faculty members, and students.

439.3 SCHOOL RESOURCE OFFICER PROGRAM

The Chief of Police should appoint SROs to serve in public primary and/or secondary schools upon contract with a Local Education Agency (LEA). The contract shall include all provisions required by Utah Code 53G-8-703.

South Salt Lake Police Department and Granite School District have entered into a School Resource Officer Interlocal Cooperation Agreement.

439.3.1 CONTRACT

See attachment: [GSD-SSL SRO Interlocal Agreement 7.29.24 \(1\).pdf](#)

439.4 SCHOOL RESOURCE OFFICER DUTIES

The general duties and responsibilities of SROs include (Utah Code 53G-8-703):

- (a) Providing for and maintaining a safe, healthy, and productive learning environment in a school.
- (b) Acting as a positive role model to students.
- (c) Working to create a cooperative, proactive, and problem-solving partnership between law enforcement and Granite School District.
- (d) Emphasizing the use of restorative approaches to address negative behavior.
- (e) Teaching a vocational law enforcement class at the request of the Granite School District/Granite Park Junior High School.

439.4.1 CHAIN OF COMMAND AND INTERNAL REPORTING

SROs should follow the chain of command and internal reporting requirements established by the [Department/Office] and the contract between the South Salt Lake Police Department and Granite School District (Utah Code 53-10-117).

439.4.2 SOUTH SALT LAKE POLICE POLICY AND PROCEDURES

All policies and procedures of the South Salt Lake Police Department, including the Use of Force, Handcuffing and Restraints, and Search and Seizure policies, are applicable to members serving as an SRO.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

School Resource Officers

439.5 SCHOOL RESOURCE OFFICER QUALIFICATIONS

Members appointed as SROs should be selected using criteria that includes but is not limited to:

- (a) The ability of the appointee to foster an optimal learning environment and educational community.
- (b) Whether the candidate has specialized training in:
 - 1. Child and adolescent development.
 - 2. De-escalation and conflict resolution techniques with children and adolescents.
 - 3. Behavioral health disorders in children and adolescents.
 - 4. Alternatives to arrest and other juvenile justice diversion strategies.
 - 5. Behavioral threat assessment methods.

439.6 TRAINING

Prior to assignment as an SRO, officers shall complete all training required by the contract (Utah Code 53G-8-703).

Members serving as an SRO shall attend the annual School Safety and Security Training Program (UAC R277-400-10).

Body-Worn Cameras

440.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the use of a body-worn camera (BWC) by members of this [department/office] and for the access, use, and retention of [department/office] BWC media (Utah Code 77-7a-102).

The provisions of this policy, including notice, documentation, access, and retention, also apply to other portable audio/video recording devices used by members, where applicable.

This policy does not apply to wiretaps or eavesdropping (concealed listening devices). Except to the extent provided in Utah Code 77-7a-104, this policy does not apply to officers engaged in undercover operations or assigned to a narcotics unit or a task force engaged primarily in narcotics investigations.

440.1.1 DEFINITIONS

Definitions related to this policy include:

Activate - To place a BWC in active mode (also called event mode). In active mode, the BWC records both video and audio.

BWC media - The video, audio, and images captured by [department/office] BWCs and the associated metadata.

BWC media systems - Any software, including web-based programs and mobile applications, used by the [Department/Office] to upload/download, store, view, transfer, and otherwise maintain BWC media.

Deactivate - To place a BWC in buffering mode (also called ready or pre-event mode). In buffering mode, the BWC records video (without audio) in short, predetermined intervals that are retained only temporarily. However, when a BWC is activated, the interval recorded immediately prior to activation is then stored as part of the BWC media. Deactivate does not mean powering off the BWC.

Event - A general term referring to a set of circumstances that may, but does not necessarily, correlate directly to a single public safety incident.

440.2 POLICY

It is the policy of the [Department/Office] to use BWCs and BWC media for evidence collection and to accurately document events in a way that promotes member safety and [department/office] accountability and transparency while also protecting the privacy of members of the public.

440.3 RESPONSIBILITIES

440.3.1 BWC COORDINATOR RESPONSIBILITIES

The Chief of Police or the authorized designee should delegate certain responsibilities to a BWC coordinator.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Body-Worn Cameras

The responsibilities of the coordinator include:

- (a) Serving as a liaison between the [Department/Office] and the BWC manufacturer/distributor and any third-party media storage vendor.
- (b) Developing inventory procedures for issuing and tracking BWC equipment, including properly marking BWCs as property of the [Department/Office] and recording the date each BWC is placed into or taken out of service.
- (c) Assisting with troubleshooting and maintenance of BWC equipment and media systems and, when necessary, coordinating the repair or replacement of BWCs.
 - 1. All equipment and system malfunctions and their resolutions should be documented, and maintenance and repair records should be maintained for all BWCs.
- (d) Managing BWC media systems so that:
 - 1. Access is limited to the minimum necessary authorized users and user privileges are restricted to those necessary for the member to conduct assigned [department/office] duties.
 - 2. Security requirements, such as two-factor authentication and appropriate password parameters, are in place for user credentials.
- (e) Configuring BWC media systems, or developing manual procedures, so that media is appropriately categorized and retained according to the event type tagged by members.
- (f) Retaining audit logs or records of all access, alteration, and deletion of BWC media and media systems, and conducting periodic audits to ensure compliance with applicable laws, regulations, and [department/office] policy.
- (g) Developing and updating BWC training for members who are assigned a BWC or given access to BWC media systems.
- (h) Coordinating with the community relations coordinator to (see the Community Relations Policy):
 - 1. Provide the public with notice of the [department/office]'s use of BWCs (e.g., posting on the [department/office] website or social media pages) (Utah Code 77-7a-105).
 - 2. Gain insight into community expectations regarding BWC use.
- (i) Coordinating with the Records Supervisor to (see the Records Section and Records Maintenance and Release policies):
 - 1. Determine and apply proper retention periods to BWC media.
 - 2. Develop procedures for the appropriate release of BWC media.
- (j) Coordinating with the Evidence Room to develop procedures for the transfer, storage, and backup of evidentiary BWC media (see the Property and Evidence Policy).
- (k) Completing an annual administrative review of the BWC program and providing it to the Chief of Police for review.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Body-Worn Cameras

440.3.2 MEMBER RESPONSIBILITIES

Every member issued a BWC is responsible for its proper use, safekeeping, and maintenance.

At the beginning of each shift or period of BWC use, the member should inspect their assigned BWC to confirm it is charged and in good working order. As part of the inspection, the member should perform a function test by activating the BWC and recording a brief video stating their name, identification number, assignment, and the date and time. The member should repeat this process at the end of each shift (Utah Code 77-7a-104).

Members should wear their assigned BWC on their outermost garment positioned at or near chest level and as close to the center of their body as practicable. Members are responsible for ensuring there are no obstructions and that the BWC remains in a position suitable for recording.

When a BWC is not in the physical possession of the member to which it is assigned, it should be placed on the charging dock and stored in a secure location.

Members shall report any malfunction or damage to the BWC coordinator or on-duty supervisor as soon as practicable and, if possible, obtain a functioning BWC to use either temporarily while repairs are being made to the member's BWC or as a permanent replacement (Utah Code 77-7a-104).

440.4 BWC USE

The following guidelines apply to the use of BWCs:

- (a) Only [department/office]-issued BWCs should be used. Members are prohibited from using any other BWC without the express consent of the Chief of Police or the authorized designee.
- (b) BWCs should only be used by the member or members to whom it was issued unless otherwise authorized by a supervisor.
- (c) The use of [department/office]-issued BWCs shall be strictly limited to [department/office]-related activities (Utah Code 77-7a-106).
 - 1. Except in exigent circumstances where it is not practicable to do so, an officer executing a search warrant shall use a BWC if one is available, (Utah Code 77-23-210).
- (d) Members shall not use BWCs or BWC media systems for which they have not received prior authorization and appropriate training.
- (e) Members shall immediately report unauthorized access or use of BWCs or BWC media systems by another member to their supervisor or the Chief of Police.

440.4.1 PROHIBITIONS

BWCs should not be used to record:

- (a) Routine administrative activities of the [Department/Office] that do not involve interactions with the public. Care should be taken to avoid incidentally recording confidential documents that the [Department/Office] has a duty to keep secure (i.e., criminal justice information).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Body-Worn Cameras

- (b) Areas within the [department/office] facilities where members have a reasonable expectation of privacy (e.g., locker rooms or dressing areas, breakrooms) unless responding to a call for service or conducting an investigation.
- (c) Conversations of other members without their knowledge.
- (d) When a member is taking an authorized break or otherwise engaged in personal activities.
- (e) In a courtroom unless responding to a call for service or emergency situation.
- (f) Interactions with undercover officers or confidential informants.
- (g) Strip searches.
- (h) Inside a hospital, health care facility, human service program, or the clinic of a health care provider except during a law enforcement encounter (Utah Code 77-7a-104).

BWCs shall not be used for the purpose of embarrassment, harassment, or ridicule of any individual or group.

440.5 ACTIVATION OF BWC

Members shall activate their BWC prior to any law enforcement encounter as defined by Utah Code 77-7a-103 (Utah Code 77-7a-104). Members are not required to activate their BWC during casual or informal contacts with members of the public that are not part of or related to law enforcement functions. However, members should activate their BWC any time a contact with an individual becomes hostile or adversarial.

Unless otherwise authorized by this policy or approved by a supervisor, BWCs shall remain activated until the law enforcement encounter has concluded (Utah Code 77-7a-104). A member may cease recording if they are simply waiting for a tow truck or a family member to arrive, or in other significant period of inactivity.

At no time is a member expected to jeopardize their safety to activate their BWC. However, the BWC should be activated as soon as reasonably practicable in required situations (Utah Code 77-7a-102; Utah Code 77-7a-104).

If a member attempts to activate their BWC but the BWC fails to record an event, the member should notify their supervisor as soon as practicable.

440.5.1 NOTICE OF RECORDING

Unless otherwise approved based on unique circumstances, a member should wear the BWC in a manner that is conspicuous and shall answer truthfully if asked whether they are equipped with a BWC or if their BWC is activated (Utah Code 77-7a-104; Utah Code 77-7a-105).

440.5.2 PRIVACY CONSIDERATIONS

Members should remain sensitive to the dignity of individuals being recorded and should exercise sound discretion with respect to privacy concerns.

Members may mute or deactivate their BWC (Utah Code 77-7a-104):

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Body-Worn Cameras

- (a) When requested by a sensitive victim of crime, a witness of a crime, or an individual who wishes to report or discuss criminal activity if the member believes that the value of the information outweighs the value of the potential recording.
- (b) During a conversation with a victim of a sexual offense or domestic violence as part of an evidence-based lethality assessment if the victim or the member believes that deactivating will encourage complete and accurate information sharing by the victim or is necessary to protect the safety or identity of the victim.
- (c) When discussing case tactics or strategy.
- (d) During private conversations with other members or emergency responders.

Members should choose to mute rather than deactivate BWCs when practicable. Deactivation should only be used when muting the BWC will not accomplish the level of privacy necessary for the situation.

Before muting or deactivating their BWC, the member should verbally narrate the reason on the recording. As soon as possible once the privacy concern is no longer an issue, or when circumstances change so that the privacy concern no longer outweighs the [department/office]'s interest in recording the event (e.g., the individual becomes combative, the conversation ends), the member should unmute or reactivate their BWC and verbally note that recording has resumed.

440.5.3 LIVESTREAMING

Livestreaming enables authorized individuals to remotely view the audio and video captured by a member's BWC in real time. Only supervisors and dispatchers approved by the Chief of Police or the authorized designee shall have access to livestreaming capabilities.

Livestreaming should only be activated:

- (a) For purposes of member safety when the member is not responding to their radio or there is some other indication of distress.
- (b) To assist with situational awareness or tactical decisions during a significant incident.
- (c) When requested by the member.

440.5.4 DOCUMENTATION

Members are encouraged to provide narration while using a BWC when it would be useful to provide context or clarification of the events being recorded. However, the use of a BWC is not a replacement for written reports and should not be referred to in a written report in place of detailing the event.

Every report prepared by a member who is issued a BWC should state "BWC available" or "BWC unavailable," as applicable, and should document (Utah Code 77-7a-104):

- (a) To the extent practicable and relevant, the identity of individuals appearing in the BWC media.
- (b) An explanation of why BWC media is unavailable including any malfunction, damage, or battery issue that resulted in the failure of the BWC to capture all or part of the event.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Body-Worn Cameras

- (c) Any exigency or other circumstances that prevented the member from immediately activating the recording at the beginning of the event.
- (d) Any period of the event in which the member deactivated or muted their BWC and the reason for such action.
- (e) If livestreaming was activated during the event, the reason for livestreaming and the members who communicated or participated in the event through BWC livestreaming.

440.6 UPLOADING BWC MEDIA

Unless otherwise authorized by a supervisor, all media from a member's BWC should be properly uploaded and tagged before the end of their shift. BWC media related to a serious or high-profile event (e.g., search for a missing child, active shooter situation) should be uploaded and tagged as soon as practicable upon returning to the [Department/Office].

Following an officer involved shooting or death or other event deemed necessary, a supervisor should take possession of the BWC for each member present and upload and tag the BWC media.

440.6.1 TAGGING BWC MEDIA

Members should tag all media captured by their BWC with their name and/or identification number, the case or incident number, and the event type. BWC media should be tagged upon uploading or, if capabilities permit tagging in the field, as close to the time of the event as possible. If more than one event type applies to BWC media, it should be tagged with each event type. If BWC media can only be tagged with a single event type, the media should be tagged using the event type with the longest retention period.

BWC media depicting sensitive circumstances or events should be tagged as restricted. BWC media should be flagged for supervisor review when it pertains to a significant event such as:

- (a) An incident that is the basis of a formal or informal complaint or is likely to result in a complaint.
- (b) When a member has sustained a serious injury or a line-of-duty death has occurred.
- (c) When a firearm discharge or use of force incident has occurred.
- (d) An event that has attracted or is likely to attract significant media attention.

Supervisors should conduct audits at regular intervals to confirm BWC media is being properly uploaded and tagged by their subordinates.

440.7 BWC MEDIA

All BWC media is the sole property of the [Department/Office]. Members shall have no expectation of privacy or ownership interest in the content of BWC media.

All BWC media shall be stored and transferred in a manner that is physically and digitally secure with appropriate safeguards to prevent unauthorized modification, use, release, or transfer. Contracts with any third-party vendors for the storage of BWC media should include provisions specifying that all BWC media remains the property of the [Department/Office] and shall not be

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Body-Worn Cameras

used by the vendor for any purpose without explicit approval of the Chief of Police or the authorized designee (Utah Code 77-7a-107).

Members shall not alter, copy, delete, release, or permit access to BWC media other than as permitted in this policy without the express consent of the Chief of Police or the authorized designee (Utah Code 77-7a-106).

BWC media systems should not be accessed using personal devices unless authorized by the Chief of Police or the authorized designee.

440.7.1 ACCESS AND USE OF BWC MEDIA

BWC media systems shall only be accessed by authorized members using the member's own login credentials and in accordance with the Information Technology Use Policy.

BWC media shall only be accessed and viewed for legitimate [department/office]-related purposes in accordance with the following guidelines:

- (a) BWC media tagged as restricted should only be accessible by those designated by the Chief of Police or the authorized designee.
- (b) Members may review their own BWC media for [department/office]-related purposes. Members should document in their report if they reviewed BWC media before completing the report.
- (c) Investigators may review BWC media pertaining to their assigned cases.
- (d) A member testifying regarding a [department/office]-related event may review the pertinent BWC media before testifying.
- (e) Supervisors are permitted to access and view BWC media of their subordinates.
 - 1. Supervisors should review BWC media that is tagged as a significant event or that the supervisor is aware pertains to a significant event.
 - 2. Supervisors should conduct documented reviews of their subordinate's BWC media at least annually to evaluate the member's performance, verify compliance with [department/office] procedures, and determine the need for additional training. The review should include a variety of event types when possible. Supervisors should review BWC media with the recording member when it would be beneficial to provide guidance or to conduct one-on-one informal training for the member.
 - 3. Supervisors should conduct periodic reviews of a sample of each subordinate's BWC media to evaluate BWC use and ensure compliance with this policy.
- (f) The Training Coordinator is permitted to access and view BWC media for training purposes.
 - 1. The Training Coordinator should conduct a quarterly review of a random sampling of BWC media to evaluate [department/office] performance and effectiveness and to identify specific areas where additional training or changes to protocols would be beneficial. Training Committee members may review BWC media as part of their review to identify training needs.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Body-Worn Cameras

2. The Training Coordinator may use BWC media for training purposes with the approval of the Chief of Police or the authorized designee. The Training Coordinator should use caution to avoid embarrassing or singling out a member and, to the extent practicable, should seek consent from the members appearing in the BWC media before its use for training. When practicable, sensitive issues depicted in BWC media should be redacted before being used for training.
- (g) The Records Supervisor may access BWC media when necessary to conduct [department/office]-related duties.
- (h) The BWC coordinator may access BWC media and the BWC media system as needed to ensure the system is functioning properly, provide troubleshooting assistance, conduct audits, and fulfill other responsibilities related to their role.

440.7.2 PUBLIC ACCESS

Unless disclosure is required by law or a court order, BWC media should not be released to the public if it unreasonably violates a person's privacy or sense of dignity or depicts the interior of:

- (a) A private residence.
- (b) A facility that offers health care, mental health or substance abuse treatment, or social services.
- (c) A school building.
- (d) Any other building in which public access is restricted or which implicates heightened security concerns.

Requests for the release of BWC media shall be processed in accordance with the Records Maintenance and Release Policy (Utah Code 77-7a-107). The Records Supervisor should review BWC media before public release.

440.8 RETENTION OF BWC MEDIA

Non-evidentiary BWC media should be retained in accordance with state records retention laws.

Unless circumstances justify continued retention, BWC media should be permanently deleted upon the expiration of the retention period in a way that it cannot be retrieved. BWC media shall not otherwise be deleted by any person without the authorization of the Chief of Police or the authorized designee.

440.8.1 EVIDENTIARY BWC MEDIA

BWC media relevant to a criminal prosecution should be exported from the BWC media system and securely transferred to digital evidence storage according to established [department/office] procedures. Evidentiary BWC media is subject to the same laws, policies, and procedures as all other evidence, including chain of custody, accessibility, and retention periods (see the Property and Evidence Policy).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Body-Worn Cameras

440.9 TRAINING

The BWC coordinator should ensure that each member issued a BWC receives initial training before use, and periodic refresher training thereafter. Training should include:

- (a) Proper use of the BWC device and accessories.
- (b) When BWC activation is required, permitted, and prohibited.
- (c) How to respond to an individual's request to stop recording.
- (d) Proper use of the BWC media systems, including uploading and tagging procedures.
- (e) Security procedures for BWC media, including appropriate access and use.

Members who are not issued a BWC but who have access to BWC media systems shall receive training on the BWC media system, including appropriate access, use, and security procedures.

Chapter 5 - Traffic Operations

Traffic

500.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for improving public safety through education and enforcement of traffic-related laws.

500.2 DEPLOYMENT

Enforcement efforts may include techniques such as geographic/temporal assignment of [department/office] members and equipment, the establishment of preventive patrols to deal with specific categories of unlawful driving, and a variety of educational activities. These activities should incorporate methods that are suitable to the situation; timed to events, seasons, past traffic problems, or locations; and, whenever practicable, preceded by enforcement activities.

Several factors will be considered in the development of deployment schedules for [department/office] members. State and local data on traffic collisions are a valuable resource. Factors for analysis include but are not limited to:

- Location.
- Time.
- Day.
- Violation factors.
- Requests from the public.
- Construction zones.
- School zones.
- Special events.

[Department/Office] members assigned to uniformed patrol or traffic enforcement functions will emphasize the enforcement of violations that contribute to traffic collisions, and also will consider the hours and locations where traffic collisions tend to occur. Members will take directed enforcement action on request and random enforcement action when appropriate. Members shall maintain high visibility while working general enforcement, especially in areas where traffic collisions frequently occur.

500.3 ENFORCEMENT

Traffic enforcement will be consistent with applicable laws and take into account the degree and severity of the violation committed. This [department/office] does not establish ticket quotas. The number of arrests or citations issued by any member shall not be used as the sole criterion for evaluating member overall performance. Several methods are effective in the reduction of traffic collisions.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Traffic

500.3.1 WARNINGS

Warnings are a non-punitive option that may be considered by the member when circumstances warrant, such as when a minor violation was inadvertent.

500.3.2 CITATIONS

Citations should be issued when a member believes it is appropriate. When issuing a citation for a traffic violation, it is essential that the rights and requirements imposed on motorists be fully explained. At a minimum, motorists should be provided with:

- (a) An explanation of the violation or charge.
- (b) The court appearance procedure, including the optional or mandatory appearance by the motorist.
- (c) A notice of whether the motorist can enter a plea and pay the fine by mail or at the court.

500.3.3 PHYSICAL ARREST

Physical arrest can be made on a number of criminal traffic offenses outlined in Utah Code Title 41. These physical arrest cases usually deal with, but are not limited to:

- (a) Vehicular manslaughter.
- (b) Felony and misdemeanor driving under the influence of alcohol/drugs.
- (c) Felony or misdemeanor hit-and-run.
- (d) Any other misdemeanor at the discretion of the officer, such as reckless driving with extenuating circumstances.

500.4 SUSPENDED OR REVOKED DRIVER'S LICENSES

If an officer contacts a traffic violator for driving on a suspended or revoked license, the officer may issue a traffic citation pursuant to Utah Code 53-3-227.

500.5 HIGH-VISIBILITY VESTS

The Department has provided American National Standards Institute (ANSI) Class II high-visibility vests to increase the visibility of department members who may be exposed to hazards presented by passing traffic, maneuvering or operating vehicles, machinery and equipment (23 CFR 655.601).

Although intended primarily for use while performing traffic related assignments, high-visibility vests should be worn at any time increased visibility would improve the safety or efficiency of the member.

500.5.1 REQUIRED USE

Except when working in a potentially adversarial or confrontational role, such as during vehicle stops, high-visibility vests should be worn when increased visibility would improve the safety of the [department/office] member or when the member will be exposed to the hazards of passing traffic or will be maneuvering or operating vehicles, machinery, and equipment.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Traffic

Examples of when high-visibility vests should be worn include traffic control duties, collision investigations, lane closures, and disaster scenes.

When emergency conditions preclude the immediate donning of the vest, members should retrieve and wear the vest as soon as conditions reasonably permit.

Use of the vests shall also be mandatory when directed by a supervisor.

500.5.2 CARE AND STORAGE

High-visibility vests shall be maintained in the trunk of each patrol and investigation vehicle, in the side box of each police motorcycle, and in the gear bag of each patrol bicycle. Each vest should be stored inside a resealable plastic bag to protect and maintain the vest in a serviceable condition. Before going into service, each employee shall ensure that a serviceable high-visibility vest is properly stored.

A supply of high-visibility vests will be maintained and made available for replacement of damaged or unserviceable vests. The Training Coordinator should be promptly notified whenever the supply of vests needs replenishing.

500.6 POLICY

It is the policy of the South Salt Lake Police Department to educate the public on traffic-related issues and to enforce traffic laws. The efforts of the [Department/Office] will be driven by such factors as the location and/or number of traffic collisions, citizen complaints, traffic volume, traffic conditions, and other traffic-related needs. The ultimate goal of traffic law enforcement and education is to increase public safety.

500.7 TRAFFIC CHECKPOINTS

Sobriety and traffic safety checkpoints may be implemented in compliance with Utah state law.

[Insert your agency's checkpoints procedures consistent with standard 25.3 requirements - see the Guide Sheet for additional guidance.]

500.8 SPEED-MEASURING DEVICES

The Traffic Sergeant is responsible for developing and maintaining procedures for using speed-measuring devices, including but not limited to:

- Operational procedures.
- Equipment specifications, care, upkeep, maintenance, and calibration.
- Operator training and certification.

[Insert your agency's procedure consistent with standard 23.5. – see the Guide Sheet for additional guidance.]

500.9 ESCORTS

Escorts of medical transport and civilian vehicles in medical emergencies are not authorized. See the Medical Aid and Response Policy for additional guidance.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Traffic

On occasion, the [Department/Office] may provide law enforcement escort services as follows:

[Insert your agency's procedure for providing escort services (e.g., funerals, parades, dignitaries, emergency vehicles, over-sized vehicles) consistent with standard 25.2. - See the Guide Sheet for additional guidance.]

500.10 TRAFFIC DIRECTION AND CONTROL

Only those [department/office] members who have received [department/office]-approved training in traffic direction and control techniques shall conduct traffic direction and control activities.

500.11 UNSAFE ROAD CONDITIONS

Unsafe road conditions due to weather, road damage, or other emergencies should be addressed as soon as practicable.

- (a) A member who locates or is assigned to investigate an unsafe road condition should use temporary traffic control devices, if necessary, to identify the safety hazard, isolate it, and limit the public's ability to come into contact with or access the area.
- (b) A member who locates or is assigned to investigate an unsafe condition should assess the condition and request through Dispatch that notifications be made to appropriate authorities responsible for correcting the safety hazard. The dispatcher should document the condition and all notifications that are made.
- (c) If a member needs assistance with isolating a safety hazard, the member may request additional members to the location.
- (d) If there are any questions regarding the proper isolation of a roadway safety hazard, members should contact their supervisor.
- (e) A member should only leave the location under one of the following circumstances:
 - 1. The unsafe condition has been corrected.
 - 2. The member is relieved by an appropriate authority who will conduct the repair, and traffic direction and control services are no longer needed.
 - 3. The member is properly relieved by another member.
 - 4. When authorized by a supervisor.

Traffic Collisions

501.1 PURPOSE AND SCOPE

This policy provides guidelines for responding to and investigating traffic collisions.

501.2 POLICY

It is the policy of the South Salt Lake Police Department to respond to traffic collisions and render or summon aid to injured victims as needed. The South Salt Lake Police Department will investigate and prepare reports according to the established minimum reporting requirements with the goal of reducing the occurrence of collisions by attempting to identify the cause of the collision and through enforcing applicable laws. Unless restricted by law, traffic collision reports will be made available to the public upon request.

501.3 RESPONSE

Upon arriving at the scene, the responding member should assess the need for additional resources and summon assistance as appropriate. Generally, the member initially dispatched to the scene will be responsible for the investigation and report, if required, unless responsibility is reassigned by a supervisor.

A supervisor should be called to the scene when the incident:

- (a) Is within the jurisdiction of this [department/office] and there is:
 - 1. A life-threatening injury.
 - 2. A fatality.
 - 3. A City vehicle involved.
 - 4. A City official or employee involved.
 - 5. Involvement of an on- or off-duty member of this [department/office].
- (b) Is within another jurisdiction and there is:
 - 1. A City of South Salt Lake vehicle involved.
 - 2. A City of South Salt Lake official involved.
 - 3. Involvement of an on-duty member of this [department/office].

501.3.1 MEMBER RESPONSIBILITIES

Upon arriving at the scene, the responding member should consider and appropriately address:

- (a) Traffic direction and control.
- (b) Proper placement of emergency vehicles, cones, roadway flares, or other devices if available to provide protection for members, the public, and the scene.
- (c) First aid for any injured parties if it can be done safely (see the Medical Aid and Response Policy).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Traffic Collisions

- (d) The potential for involvement of hazardous materials (see the Hazardous Material Response Policy).
- (e) The need for additional support as necessary (e.g., traffic control, emergency medical services, fire department, hazardous materials response, tow vehicles).
 - 1. The fire department shall be immediately summoned for any fire hazard at the scene of a collision. Members should take all reasonable measures to protect collision victims and themselves from fire injury.
- (f) Clearance and cleanup of the roadway.

501.4 NOTIFICATION

If a traffic collision involves a life-threatening injury or fatality, the responding officer shall notify a supervisor or, if unavailable, the Watch Commander. The Watch Commander or any supervisor may assign a traffic investigator or other appropriate personnel to investigate the incident. The Watch Commander will ensure notification is made to the Traffic Sergeant, command staff, Deputy Chief and Chief in accordance with the Major Incident Notification Policy.

501.4.1 NOTIFICATION OF FAMILY

In the event of a life-threatening injury or fatality, the supervisor responsible for the incident should ensure notification of the victim's immediate family or coordinate such notification with the medical examiner, victim advocate, or another suitable person. Notification should be made as soon as practicable following positive identification of the victim.

The identity of any person seriously injured or deceased in a traffic collision should not be released until notification is made to the victim's immediate family.

501.5 MINIMUM REPORTING REQUIREMENTS

A collision report shall be taken when (Utah Code 41-6a-402):

- (a) A fatality, any injury (including complaint of pain), driving under the influence, or hit-and-run is involved.
- (b) An on-duty member of the City of South Salt Lake is involved.
- (c) The collision results in any damage to any City-owned or leased vehicle.
- (d) The collision involves any other public agency driver or vehicle.
- (e) There is damage to public property.
- (f) There is damage to any vehicle to the extent that towing is required.
- (g) Prosecution or follow-up investigation is contemplated.
- (h) Directed by a supervisor.
- (i) A report is requested by any involved driver.
- (j) There is total property damage that appears to exceed \$2,500.
- (k) Must be filed within 10 days after the request.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Traffic Collisions

501.5.1 PRIVATE PROPERTY

Traffic collision reports shall be taken for traffic collisions occurring on private property when the collision results in injury to or death of any person or total property damage appears to exceed \$2,500 (Utah Code 41-6a-402). An incident report may also be taken at the discretion of any supervisor.

501.5.2 CITY VEHICLE INVOLVED

A traffic collision report shall be taken when a City vehicle is involved in a traffic collision that results in property damage or injury.

A general information report may be taken in lieu of a traffic collision report at the direction of a supervisor when the incident occurs entirely on private property or does not involve another vehicle.

Whenever there is damage to a City vehicle, a vehicle damage report shall be completed and forwarded to the appropriate Division Commander. The traffic investigator or supervisor at the scene should determine what photographs should be taken of the scene and the vehicle damage.

501.5.3 INJURED ANIMALS

South Salt Lake Police officers should contact Animal Control when a traffic collision involves the disposition of an injured animal.

501.5.4 TRAFFIC COLLISIONS INVOLVING LIVESTOCK

An officer investigating a collision shall indicate in the report whether the collision occurred on a highway designated as a livestock highway, in accordance with Utah Code 72-3-112, when the collision resulted in the injury or death of livestock (Utah Code 41-6a-404).

An officer investigating such a collision shall make reasonable efforts as soon as practicable to (Utah Code 41-6a-408):

- (a) Locate and inform the owner of the livestock of the incident.
- (b) Make arrangements with the owner of the livestock to provide a copy of the collision report or advise the owner where a copy can be obtained.

501.6 INVESTIGATION

When a traffic collision meets minimum reporting requirements the investigation should include, at a minimum:

- (a) Identification and interview of all involved parties.
- (b) Identification and interview of any witnesses.
- (c) A determination of whether a violation of law has occurred and the appropriate enforcement action.
- (d) Identification and protection of items of apparent evidentiary value.
- (e) Documentation of the incident as necessary (e.g., statements, measurements, photographs, collection of evidence, reporting) on the appropriate forms.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Traffic Collisions

501.6.1 INVESTIGATION BY OUTSIDE LAW ENFORCEMENT AGENCY

The Traffic Sergeant or on-duty Watch Commander should request that the Utah Highway Patrol or other outside law enforcement agency investigate and complete a traffic collision investigation when a life-threatening injury or fatal traffic collision occurs within the jurisdiction of the and involves:

- (a) An on- or off-duty member of South Salt Lake City..
 - 1. The involved member shall complete the necessary traffic collision forms. If the member is unable to complete the form, the supervisor shall complete it.
- (b) An on- or off-duty official or employee of the City of South Salt Lake.

Any South Salt Lake City Police Department members shall promptly notify a supervisor when any South Salt Lake City vehicle is involved in a traffic collision. The collision investigation and report shall be completed by the agency having jurisdiction.

501.7 ENFORCEMENT ACTION

After a thorough investigation in which physical evidence or independent witness statements indicate that a violation of a traffic law contributed to the collision, authorized members should issue a citation or arrest the offending driver, as appropriate.

More serious violations, such as driving under the influence of drugs or alcohol, vehicular manslaughter, or other felonies, shall be enforced. If a driver who is subject to enforcement action is admitted to a hospital, a supervisor shall be contacted to determine the best enforcement option.

501.7.1 TRAFFIC COLLISIONS INVOLVING SERIOUS INJURY OR DEATH

An officer who issues a citation to a person for a moving traffic violation that results in a collision causing serious bodily injury or death shall note that fact on the citation (Utah Code 41-6a-202).

501.8 REPORTS

Members shall utilize forms approved by the Utah Department of Transportation (UDOT) as required for the reporting of traffic collisions. All such reports shall be forwarded to the Traffic Sergeant for approval and filing.

501.8.1 REPORT MODIFICATION

A change or modification of a written report that alters a material fact in the report may be made only by the member who prepared the report, and only prior to its approval and distribution. Once a report has been approved and distributed, corrections shall only be made by way of a written supplemental report. A written supplemental report may be made by any authorized member.

501.9 REVIEW OF SOUTH SALT LAKE VEHICLE-INVOLVED COLLISIONS

South Salt Lake Personnel Policies and Procedures Manual: Section XV: General Safety 5. Motor Vehicle Accident Prevention Procedure.

501.10 TRAFFIC SERGEANT RESPONSIBILITIES

The responsibilities of the Traffic Sergeant include but are not limited to:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Traffic Collisions

- (a) Ensuring the monthly and quarterly reports on traffic collision information and statistics are forwarded to the Patrol Division Commander or other persons as required.
- (b) Distribution of the Collision Investigation Manual. The Traffic Sergeant will receive all changes in the state manual and ensure conformity with this policy.

Vehicle Towing

502.1 PURPOSE AND SCOPE

This policy provides guidance related to vehicle towing.

502.2 TOWING SERVICES

Members shall not show preference among towing services that have been authorized for use by the [Department/Office]. A rotation or other system established by the [Department/Office] for tow services should be followed.

502.3 VEHICLE INVENTORY

The contents of all vehicles towed at the request of [department/office] members shall be inventoried and listed on the inventory report. When reasonably practicable, photographs may be taken to assist in the inventory.

- (a) An inventory of personal property and the contents of open containers will be conducted throughout the passenger and engine compartments of the vehicle including but not limited to any unlocked glove box, other accessible areas under or within the dashboard area, any pockets in the doors or in the back of the front seat, in any console between the seats, under any floor mats, and under the seats.
- (b) In addition to the passenger and engine compartments as described above, an inventory of personal property and the contents of open containers will also be conducted in any other type of unlocked compartments that are a part of the vehicle, including unlocked vehicle trunks and unlocked car top containers.
- (c) Any locked compartments including but not limited to locked glove compartments, locked vehicle trunks, locked hatchbacks, and locked car-top containers should be inventoried, provided the keys are available and released with the vehicle to the third-party towing company or an unlocking mechanism for such compartment is available within the vehicle.
- (d) Closed containers located either within the vehicle or any of the vehicle's compartments will not be opened for inventory purposes except for the following: wallets, purses, coin purses, fanny packs, personal organizers, briefcases or other closed containers designed for carrying money, small valuables, or hazardous materials.

Members should ask the occupants whether the vehicle contains any valuables or hazardous materials. Responses should be noted in the inventory report. If the occupant acknowledges that any closed container contains valuables or a hazardous material, the container shall be opened and inventoried. When practicable and appropriate, such items should be removed from the vehicle and given to the owner, or booked into property for safekeeping.

Any cash, jewelry, or other small valuables located during the inventory process will be held for safekeeping, in accordance with the Property and Evidence Policy. A copy of the property receipt form should be given to the person in control of the vehicle or, if that person is not present, left in the vehicle.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Towing

A copy of the vehicle inventory will be given to the tow truck operator.

These inventory procedures are for the purpose of protecting the vehicle owner's property, providing for the safety of [department/office] members, and protecting the [Department/Office] against fraudulent claims of lost, stolen, or damaged property.

Towing a vehicle in order to perform an inventory should not be used as a pretext for an evidence search. Nothing in this policy prevents the towing of a vehicle that would occur for reasons independent of any suspicion that the vehicle may contain evidence if it is otherwise justified by law or this policy.

502.4 SECURITY OF VEHICLES AND RETRIEVAL OF PROPERTY

If the search of a vehicle leaves the vehicle or any property contained therein vulnerable to unauthorized entry, theft, or damage, the [department/office] member conducting the search shall take such steps as are reasonably necessary to secure or protect the vehicle or property from such hazards.

Unless it would cause an unreasonable delay in the completion of a vehicle impound/storage or create an issue of officer safety, reasonable accommodations should be made to permit the owner, operator, or occupant to retrieve small items of value or personal need (e.g. cash, jewelry, cell phone, prescriptions) that are not considered evidence or contraband.

Members who become aware that a vehicle may have been towed by the [Department/Office] in error should promptly advise a supervisor. Supervisors should approve, when appropriate, the release of the vehicle without requiring the owner or the owner's agent to request a hearing to contest the tow.

502.5 POLICY

The South Salt Lake Police Department will tow vehicles when appropriate and in accordance with the law.

502.6 REMOVAL OF VEHICLES DUE TO HAZARD

When a vehicle should be towed because it presents a hazard, the owner or operator should arrange for the towing. [Department/Office] members may assist by communicating requests through Dispatch to expedite the process.

If the owner or operator is unable to arrange for towing and the vehicle presents a hazard, the vehicle may be towed at the direction of the [department/office] member (Utah Code 41-6a-1405).

Vehicles that are not the property of the City should not be driven by [department/office] members unless it is necessary to move the vehicle a short distance to eliminate a hazard, prevent the obstruction of a fire hydrant, or comply with posted signs.

502.6.1 REMOVAL OF VEHICLE INVOLVED IN AN ACCIDENT

An officer may, without the consent of the owner, remove a vehicle that has been involved in an accident if the vehicle has been damaged or spilled within the right-of-way or any portion of a

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Towing

roadway on the state highway system, is blocking a roadway, or is otherwise endangering public safety (Utah Code 41-6a-401.9).

502.6.2 REMOVAL OF ABANDONED VEHICLES

A vehicle is considered abandoned and may be removed by an officer if it has been left unattended more than 48 hours on a highway or more than seven days on public or private property without the property owner's consent (Utah Code 41-6a-1408).

502.7 ARREST SCENES

Whenever the owner or operator of a vehicle is arrested, the arresting officer should provide reasonable safekeeping by leaving the vehicle secured and lawfully parked at the scene or, when appropriate, by having the vehicle towed, such as when the vehicle presents a traffic hazard or the vehicle would be in jeopardy of theft or damage if left at the scene (Utah Code 41-6a-1405).

Officers are not required to investigate whether alternatives to towing a vehicle exist after an arrest. However, a vehicle should not be towed if reasonable alternatives exist. When considering whether to leave a vehicle at the scene, officers should take into consideration public safety as well as the reasonable safety of the vehicle and its contents.

The following are examples of situations where a vehicle should not be towed:

- (a) The vehicle can be legally parked, left in a reasonably secure and safe location, and is not needed as evidence.
- (b) The vehicle is parked on private property, on which the arrestee or owner is legally residing, or the property owner does not object to the vehicle being parked at that location.
- (c) The arrestee or owner of the vehicle requests that it be released to a person who is present, willing, and able to legally take control of the vehicle.
- (d) The vehicle is legally parked and the arrestee or owner requests that it be left at the scene. In such cases the requester should be informed that the [Department/Office] will not be responsible for theft or damages.

502.7.1 IMPOUND FOR LACK OF PROOF OF SECURITY

If the operator of a vehicle involved in a collision cannot provide proof of security as required by Utah Code 41-12a-301, the vehicle shall be impounded after the officer confirms that the security is not in effect through a query of the Uninsured Motorist Identification Database (Utah Code 41-1a-1101).

502.7.2 IMPOUND FOR ROAD RAGE EVENT

When an officer has probable cause to believe the operator of a vehicle has engaged in a road rage event and the operator has been arrested in conjunction with that event, the officer shall impound the vehicle unless the registered owner is someone other than the operator and is present to take possession of the vehicle (Utah Code 41-1a-1101).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Towing

502.8 VEHICLES RELATED TO CRIMINAL INVESTIGATIONS

Officers should tow vehicles that are needed for the furtherance of an investigation or prosecution of a case, or that are otherwise appropriate for seizure as evidence. Officers should make reasonable efforts to return a recovered stolen vehicle to its owner rather than have it towed, so long as the vehicle is not needed for evidence.

502.9 RECORDS

Records Section members shall ensure that pertinent data regarding a towed vehicle is promptly entered into the appropriate database.

502.9.1 VEHICLE IMPOUND REPORT

[Department/Office] members towing a vehicle shall complete a Vehicle Impound Report in the format approved by the Motor Vehicle Division. The report should be submitted to the Records Section as soon as practicable after the vehicle is towed.

The [Department/Office] shall forward the Vehicle Impound Report, containing all required information, to the Motor Vehicle Division before noon on the next business day after the date of the impoundment (Utah Code 41-6a-1406(4)).

502.9.2 INFORMATION TO TOW TRUCK DRIVER

When an officer has a vehicle removed but not impounded, the officer shall provide the tow truck operator with their name and badge number, the name and originating agency identifier of the [Department/Office], and the [department/office] case number (Utah Code 41-6a-1406(5)).

502.10 STORAGE OF VEHICLES

A vehicle being impounded shall be stored at a state impound yard. A vehicle being removed but not impounded shall be stored at a state impound yard unless the registered owner has requested a different location and made payment to the tow truck operator at the time of removal (Utah Code 41-6a-1406).

Impaired Driving

503.1 PURPOSE AND SCOPE

This policy provides guidance to those [department/office] members who play a role in the detection and investigation of driving under the influence (DUI).

503.2 POLICY

The South Salt Lake Police Department is committed to the safety of the roadways and the community and will pursue fair but aggressive enforcement of Utah's impaired driving laws.

503.3 FIELD TESTS

The Traffic Sergeant should identify standardized FSTs and any approved alternate tests for officers to use when investigating violations of DUI laws. The National Highway Traffic Safety approved Standard Field Sobriety Test are the testing standard.

503.3.1 ORAL FLUID AND PORTABLE BREATH TESTING

A voluntary oral fluid test or portable breath test may be administered in accordance with UAC R714-501-3 and UAC R714-501-4 if there is evidence of impairment based on the totality of the circumstances after the FSTs have been administered. The oral fluid or portable breath test shall not be the primary factor upon which a decision to arrest is made.

503.4 CHEMICAL TESTS

A person implies consent under Utah law to a chemical test or tests, and to providing the associated chemical sample, under any of the following (Utah Code 41-6a-520):

- (a) The officer has reasonable grounds to believe that the person was operating or in actual physical control of a motor vehicle while:
 - 1. Having a prohibited blood or breath alcohol content level as defined by Utah Code 41-6a-502 (DUI) or Utah Code 41-6a-530 (Alcohol Restricted Drivers).
 - 2. Under the influence of alcohol, any drug or combination of alcohol and any drug.
 - 3. Having any measurable controlled substance or metabolite of a controlled substance in the person's body.
- (b) The officer has stopped a person under the age of 21 and has reasonable grounds to believe that the person was operating or in actual physical control of a vehicle or motorboat with a measurable blood, breath or urine alcohol concentration in the person's body (Utah Code 53-3-231).

If a person withdraws this implied consent, or is unable to withdraw consent (e.g., the person is unconscious), the officer should consider implied consent revoked and proceed as though the person has refused to provide a chemical sample.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Impaired Driving

503.4.1 BREATH SAMPLES

The Traffic Sergeant should ensure that all devices used for the collection and analysis of breath samples are properly serviced and tested, and that a record of such service and testing is properly maintained.

Officers obtaining a breath sample should monitor the device for any sign of malfunction. Any anomalies or equipment failures should be noted in the appropriate report and promptly reported to the Traffic Sergeant.

503.4.2 BLOOD SAMPLES

Only persons authorized by law to draw blood shall collect blood samples (Utah Code 41-6a-523; Utah Code 77-23-213). The blood draw should be witnessed by the assigned officer. No officer, even if properly certified, should perform this task.

Officers should inform an arrestee that if he/she chooses to provide a blood sample, a separate sample can be collected for alternate testing. Unless medical personnel object, two samples should be collected and retained as evidence, so long as only one puncture is required.

The blood sample shall be packaged, marked, handled, stored, and transported as required by the testing facility.

If an arrestee cannot submit to a blood draw because he/she has a bleeding disorder or has taken medication that inhibits coagulation, he/she shall not be required to take a blood test. Such inability to take a blood test should not be considered a refusal. However, that arrestee may be required to complete another available and viable test.

503.4.3 URINE SAMPLES

If a urine test will be performed, the arrestee should be promptly transported to the appropriate testing site. The officer shall follow any directions accompanying the urine evidence collection kit.

Urine samples shall be collected and witnessed by an officer or jail staff member of the same sex as the person giving the sample. The arrestee tested should be allowed sufficient privacy to maintain his/her dignity, to the extent possible, while still ensuring the accuracy of the sample.

The sample shall be packaged, marked, handled, stored and transported as required by the testing facility.

503.4.4 STATUTORY NOTIFICATIONS

An officer requesting that a person submit to a chemical test shall provide the person with a mandatory warning pursuant to Utah Code 41-6a-520.

503.5 REFUSALS

When an arrestee refuses to provide a chemical sample, officers should:

- (a) Advise the arrestee of the requirement to provide a sample (Utah Code 41-6a-520).
- (b) Audio- and/or video-record the admonishment and the response when it is practicable.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Impaired Driving

- (c) Document the refusal in the appropriate report.

503.5.1 STATUTORY NOTIFICATIONS UPON REFUSAL

Upon refusal to submit to a chemical test as required by law, officers shall personally serve the notice of the Driver License Division's (DLD) intention to revoke the person's driving privilege or license upon the person (Utah Code 41-6a-520).

503.5.2 BLOOD SAMPLE WITHOUT CONSENT

A blood sample may be obtained from a person who refuses a chemical test when any of the following conditions exist (Utah Code 77-23-213):

- (a) A search warrant has been obtained.
- (b) The officer can articulate that exigent circumstances exist. Exigency does not exist solely because of the short time period associated with the natural dissipation of alcohol or controlled or prohibited substances in the person's bloodstream. Exigency can be established by the existence of special facts, such as a lengthy time delay resulting from an accident investigation or medical treatment of the person.

503.5.3 FORCED BLOOD SAMPLE

If an arrestee indicates by word or action that he/she will physically resist a blood draw, the officer should request a supervisor to respond.

The responding supervisor should:

- (a) Evaluate whether using force to obtain a blood sample is appropriate under the circumstances.
- (b) Ensure that all attempts to obtain a blood sample through force cease if the person agrees to, and completes, a viable form of testing in a timely manner.
- (c) Advise the person of his/her duty to provide a sample (even if this advisement was previously done by another officer), and attempt to persuade the individual to submit to such a sample without physical resistance. This dialogue should be recorded on audio and/or video when practicable.
- (d) Ensure that the blood sample is taken in a medically approved manner.
- (e) Ensure that the forced blood draw is recorded on audio and/or video when practicable.
- (f) Monitor and ensure that the type and level of force applied appears reasonable under the circumstances.
 - 1. Unless otherwise provided in a warrant, force should generally be limited to handcuffing or similar restraint methods.
 - 2. In misdemeanor cases, if the arrestee becomes violent or more resistant, no additional force will be used and a refusal should be noted in the report.
 - 3. In felony cases, force which reasonably appears necessary to overcome the resistance to the blood draw may be permitted.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Impaired Driving

- (g) Ensure the use of force and methods used to accomplish the collection of the blood sample are documented in the related report.

If a supervisor is unavailable, officers are expected to use sound judgment and perform as a responding supervisor, as set forth above.

503.6 ARREST AND INVESTIGATION

503.6.1 ARREST AUTHORITY

An officer may make a warrantless arrest of a person that the officer has probable cause to believe has violated the DUI laws of this state, whether or not the offense occurred in the officer's presence (Utah Code 41-6a-508).

503.6.2 OFFICER RESPONSIBILITIES

An officer serving a person with a notice of the DLD intention to revoke the person's driving privilege or license shall also (Utah Code 41-6a-520):

- (a) Provide the person with basic information regarding how to obtain a hearing before DLD.
- (b) Forward a report to DLD within 10 days of giving the notice to the person that the officer had reasonable grounds to believe the arrested person was DUI and that the person refused to submit to a chemical test as required by law.

503.6.3 VEHICLE IMPOUNDMENT

An officer who arrests a person for DUI shall seize and impound the vehicle the person was driving at the time of the arrest. If operable, the vehicle may be released upon request to the registered owner of the vehicle if the person is able to present proof of ownership, a valid driver license and that the person would not be in violation of the DUI laws of this state if permitted to operate the vehicle (Utah Code 41-6a-527).

503.6.4 SELECTION OF CHEMICAL TEST

The investigating officer shall determine which chemical test or tests to administer to a person and how many tests will be administered. In the event that an officer requests that the person submit to more than one test, refusal by the person to take one or more of the requested tests, even if the person has already submitted to one test, is nonetheless considered a refusal under state DUI laws (Utah Code 41-6a-520).

503.6.5 ADDITIONAL TESTING

A person may have qualified medical personnel administer an additional test, at the person's own expense. The additional test shall be administered subsequently to that which is administered at the direction of the officer (Utah Code 41-6a-520).

503.7 REPORTING

The Traffic Sergeant in conjunction with the Crime Analyst shall ensure that the [Department/Office] complies with all reporting requirements pursuant to Utah Code 53-10-206.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Impaired Driving

Effective 5/7/2025

53-10-206 Collection of Information.

The commissioner and persons designated by the commissioner may require all peace officers, the warden of the state prison, the keeper of any jail or correctional institution, or superintendent of the state hospital to obtain information that will aid in establishing the records required to be kept.

503.7.1 CRASH AND ARREST DATA

The Traffic Sergeant in conjunction with the Crime Analyst should facilitate the collection of information from officers required by Utah Code 53-10-118 for submission to the Criminal Investigations and Technical Services Division (Utah Code 53-25-104). Effective 5/7/2025 53-25-104. Driving Under the Influence Reporting Requirements. Beginning on January 1, 2026, a law enforcement agency shall collect and provide to the departments's Criminal Investigations and Technical Services Division the driving under the influence crash and arrest data described in Section 53-10-118.

Effective 5/7/2025

53-10-118. Collection of Driving Under the Influence Crash and Arrest Data

(1) (a) The division shall collect from every law enforcement agency the following data concerning a crash that appears to be connected with the driving under the influence offense:

- (i) whether the impaired driver was injured or killed
- (ii) whether any other individual was injured or killed
- (iii) whether there was damaged to real or personal property;
- (iv) the following results or findings regarding the impaired driver's impairment:
 - (A) blood, breath, or urine alcohol concentration readings; and
 - (B) blood, urine, chemical, or similar tests detecting alcohol or other drugs in an individual; and
- (v) if applicable, the name of the establishment that provided the alcohol to the impaired driver.

(b) The division shall collect from every law enforcement agency the following data for every arrest made for the suspected driving under the influence offense, including those that are unrelated to a crash described in Subsection (1)(a):

- (i) the data described in Subsections (1)(a)(iv) and (v); and
- (ii) if there were any injuries, deaths, or property damage based on the driving under the influence incident, a description of the injuries, death, or damages.

(c) In accordance with Section 53-25-104, a law enforcement agency shall provide the information described in Subsections (1)(a) and (b) in the form and manner requested by the division.

(2) The division shall provide the information collected under Subsection (1) to the Commission on Criminal Juvenile Justice for use in the annual report described in Section 41-6a-511.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Impaired Driving

503.8 RECORDS BUREAU RESPONSIBILITIES

The Records Supervisor will ensure that all case-related records are transmitted according to current records procedures and as required by the prosecuting attorney's office.

503.9 ADMINISTRATIVE HEARINGS

The Records Supervisor will ensure that all appropriate reports and documents related to administrative license suspensions are reviewed and forwarded to DLD.

Any officer who receives notice of required attendance to an administrative license suspension hearing should promptly notify the prosecuting attorney.

An officer called to testify at an administrative hearing should document the hearing date and DLD file number in a supplemental report. Specific details of the hearing generally should not be included in the report unless errors, additional evidence or witnesses are identified.

503.10 TRAINING

The Training Coordinator should ensure that officers participating in the enforcement of DUI laws receive regular training. Training should include, at minimum, current laws on impaired driving, investigative techniques, and rules of evidence pertaining to DUI investigations. The Training Coordinator shall also ensure that each officer receives training on the current standard field sobriety testing guidelines established by National Highway Traffic Safety Administration and on the proper use of oral fluid and portable breath tests (Utah Code 41-6a-515.6; Utah Code 53-25-102; UAC R714-501-3; UAC R714-501-4).

The Training Coordinator should confer with the prosecuting attorney's office and update training topics as needed.

Traffic Citations

504.1 PURPOSE AND SCOPE

This policy outlines the responsibility for traffic citations, the procedure for dismissal, correction and voiding of traffic citations.

504.2 RESPONSIBILITIES

The Traffic Sergeant shall be responsible for the development and design of all Department traffic citations in compliance with state law and the Judicial Council.

The Records Section shall be responsible for the supply and accounting of all traffic citations issued to employees of the Department.

504.3 DISMISSAL OF TRAFFIC CITATIONS

Employees of the Department do not have the authority to dismiss a citation once it has been issued. Only the court has the authority to dismiss a citation that has been issued (Utah Code 77-7-26). Any request from a recipient to dismiss a citation shall be referred to the Watch Commander directly supervising the issuing officer. Upon a review of the circumstances involving the issuance of the traffic citation, the Watch Commander may request the affected Division Commander to recommend dismissal of the traffic citation. If approved, the citation will be forwarded to the appropriate court with a request for dismissal. All recipients of traffic citations whose request for the dismissal of a traffic citation has been denied shall be referred to the appropriate court.

Should an officer determine during a court proceeding that a traffic citation should be dismissed in the interest of justice or where prosecution is deemed inappropriate the officer may request the court to dismiss the citation. Upon dismissal of the traffic citation by the court, the officer shall notify his/her immediate supervisor of the circumstances surrounding the dismissal and shall complete any paperwork as directed or required. The citation dismissal shall then be forwarded to the officers assigned Division Commander for review.

504.4 VOIDING TRAFFIC CITATIONS

Voiding a traffic citation may occur when a traffic citation has not been completed or where it is completed but not issued. All copies of the citation shall be presented to a supervisor to approve the voiding of the citation. The citation and copies shall then be forwarded to the Records Division.

504.5 CORRECTION OF TRAFFIC CITATIONS

When a traffic citation is issued and in need of correction, the officer issuing the citation shall submit the citation and a letter requesting a specific correction to his/her immediate supervisor. The citation and letter shall then be forwarded to the South Salt Lake City Attorneys Office.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Traffic Citations

504.6 DISPOSITION OF TRAFFIC CITATIONS

The court and file copies of all traffic citations issued by members of the Department shall be forwarded to the employee's immediate supervisor for review. The citation copies shall then be filed with the Records Section.

Upon separation from employment with the department, all employees issued traffic citations books shall return any unused citations to their direct supervisor

504.7 JUVENILE CITATIONS

Completion of traffic citation forms for juveniles may vary slightly from the procedure for adults. The juvenile's age, place of residency and the type of offense should be considered before issuing the juvenile a citation.

Disabled Vehicles

505.1 PURPOSE AND SCOPE

All law enforcement agencies having responsibility for traffic enforcement should develop and adopt a written policy to provide assistance to motorists in disabled vehicles within the Department's primary jurisdiction.

505.2 OFFICER RESPONSIBILITY

When an on-duty officer observes a disabled vehicle on the roadway, the officer should make a reasonable effort to provide assistance. If that officer is assigned to a call of higher priority, the dispatcher should be advised of the location of the disabled vehicle and the need for assistance. The dispatcher should then assign another officer to respond for assistance as soon as practical.

An officer may remove a vehicle that has been involved in a collision (or property from within the vehicle) without the consent of the owner if it is blocking a roadway or is otherwise endangering public safety (Utah Code 41-6a-401.9).

505.3 EXTENT OF ASSISTANCE

In most cases, a disabled motorist will require assistance. After arrangements for assistance are made, continued involvement by Department personnel will be contingent on the time of day, the location, the availability of Department resources and the vulnerability of the disabled motorist.

505.3.1 MECHANICAL REPAIRS

Department personnel shall not make mechanical repairs to a disabled vehicle. The use of push bumpers to relocate vehicles to a position of safety is not considered a mechanical repair.

505.3.2 RELOCATION OF DISABLED VEHICLES

The relocation of disabled vehicles by members of this department by pushing or pulling a vehicle should only occur when the conditions reasonably indicate that immediate movement is necessary to reduce a hazard presented by the disabled vehicle.

505.3.3 RELOCATION OF MOTORIST

The relocation of a motorist with a disabled vehicle should only occur with the person's consent and should be suggested when conditions reasonably indicate that immediate movement is necessary to mitigate a potential hazard. The department member may stay with the disabled motorist or transport him/her to a safe area to await pickup.

505.4 PUBLIC ACCESS TO THIS POLICY

This policy is available upon request.

CHECKPOINTS

Effective Date:	
Revised Date:	
Issuing Authority: South Salt Lake PD	

506.1 PURPOSE

The purpose of the policy is to establish the use of administrative checkpoints as viable methods that may be used by the department in both planned and unplanned situations.

506.2 POLICY

Members of the south Salt Lake Police Department will conduct administrative checkpoints in accordance with Utah's Administrative Traffic Checkpoint Act (Title 77, Section 23, Part 1) and applicable decisions by federal and state courts.

506.3 DEFINITIONS

The following definitions are found in Utah Code 77-23-102

Administrative Traffic Checkpoint-A roadblock procedure where enforcement officers shall stop all, or a designated sequence of, motor vehicle traveling on highways and roads and subject those vehicles to inspection to testing the drivers or occupants to questioning or the production of documents.

Command Level Officer-Includes all sheriffs, heads of law enforcement agencies, agencies and all supervisory enforcement officer of sergeant rank or higher.

Emergency Circumstances-Circumstances where enforcement officers reasonably believe road conditions, weather conditions, or persons present a significant hazard to persons or the property of other persons.

506.4 ADMINISTRATIVE TRAFFIC CHECKPOINTS

506.4.1 PLANNED ADMINISTRATIVE TRAFFIC CHECKPOINTS

Planned administrative traffic checkpoints shall have the primary purpose of inspecting, verifying, or detecting one or more of the following:

- Drivers that may be under the influence of alcohol or drugs;
- License plates, registration certificates, insurance certificates or drivers licenses
- Violations of Title 23. Wildlife Resources Code of Utah; or
- Other circumstances that are specifically distinguishable, by the magistrate, from a general interest in crime control.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

CHECKPOINTS

Planned administrative traffic checkpoints require a written plan, approval of the Deputy Chief, authorization for filing by a City or County Prosecutor, and written authority of a magistrate.

Additional requirements can be found in Utah Code 77-23-104

The Utah Highway Safety Office shall be consulted about any planned administrative traffic checkpoints.

Following the completion of a planned administrative traffic checkpoint, the coordinating sworn member will be responsible for assembling an after-action report for review by the Chief of Police. The after-action report will include maps, the original written plan, signed authorization from a magistrate, all associated police reports, statistical information, enforcement information, justification for any deviation from the original written plan, advanced notice to the public and any recommendations for improvement for future planned administrative traffic checkpoints. This will be completed within ten (10) days following the planned event.

506.5 UNPLANNED ADMINISTRATIVE TRAFFIC CHECKPOINTS

Utah Code 77-23-103 gives enforcement officers the authority to conduct unplanned administrative traffic checkpoints in emergency circumstances. Unplanned administrative traffic checkpoints must be authorized by the Deputy Chief and written authority from a magistrate shall be sought as soon as possible.

Situations when an unplanned administrative traffic checkpoint might be used include, but are not limited to:

- Apprehension of a violent fugitive
- Kidnappings or AMBER Alert Investigation
- Acts of Terrorism

Sworn members will consider the seriousness of the specific event or situation in determining:

(a) In an unplanned administrative traffic checkpoint should be implemented or maintained;

(b) The strategic location(s) for an unplanned administrative traffic checkpoint;

1. Strategic locations (highway intersections, bridges, along natural barriers, exits to subdivisions and apartments) to contain suspect(s) in a defined area and facilitate apprehension.

(c) The extent to which access will be blocked (totally or partially):

(d) The resources available and necessary to implement an effective unplanned administrative traffic checkpoint;

(e) How access will be blocked (traffic cones, signs, patrol vehicles, or other barricades).

1. Members using their marked patrol vehicles as barricades, or parking their marked vehicles contrary to statutory requirements, will have emergency lights activated, position vehicle to promote safety and gain the best tactical advantage for the situation, and will not remain in the vehicles.

Motorcycle Officer Program

507.1 PURPOSE AND SCOPE

It is the policy of this department to prepare police officers with the additional skill required in the operation of a two wheel motorcycle while performing enforcement duty or motorcycle instruction, and to select officers by established standards and training.

Under no circumstances will anyone operate a department motorcycle without a DOT- and department-approved safety helmet properly secured to the officer's head.

507.1.1 ASSIGNMENTS

A three (3) year commitment will be required in the Motor Division, with a five (5) year maximum.

(a) Motor Officer categories and criteria defined:

1. Level 1 Motor Officer (Primary Assignment).

- (a) Police officer currently assigned to the Motor Unit.
- (b) Police officer currently certified by this department as a police motorcycle rider.
- (c) Police officer who has maintained a police motorcycle ride certification through standards and training as designated by the South Salt Lake Police Department.

2. Level 2 Motor Officer (Alternate Assignment).

- (a) Police officer chosen by Department administration to fill a temporary position in the Motor Unit. If and when that position becomes permanent, and all other required criteria is met, the officer will be upgraded to Level 1.
- (b) Police officer who maintains a valid Utah Motorcycle Operators License.

(b) Training and Certification:

(a) Level 1 officers may retain the Level 1 status for a period of six months if one of the following conditions restrict the officer from regular Motor operation:

- (a) Injury and/or mental or physical illness.
- (b) Temporary administrative transfer from the Motor Unit or motor operation.
- (c) Leave of absence, vehicle shortage, extensive training, or other reason as designated by the Chief of Police or his/her designee.

(b) Absence Certification Requirements:

- (a) Level 1 and 2 officers may be required to participate in regular motor training depending on the absence circumstances.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Motorcycle Officer Program

- (b) If absence of regular motor operation and training is one year or greater, the officer will be required to successfully complete a re-certification program of training as designated by the South Salt Lake City Police Department.
 - (a) If the absence is greater than one year, the reasons and conditions of absence will be reviewed by the Motor Sergeant and the Department administration.
 - (b) If necessary, the Traffic Unit Commander may authorize that the officer be transferred from the Motor Unit if such transfer is found to be in the best interests of the Department.
 - (c) The officer will be provided with information as it relates to the administration review and reasons for transfer, and may exercise his or her rights to a hearing, etc.
 - (c) If absence of regular motor operation and training is eighteen months or greater, the officer will be required to successfully complete the initial certification training as designated by the South Salt Lake City Police Department.
- (c) Assignments:
 - (a) Due to the special skills and hazards involved in motorcycle operation, officers assigned to motorcycle duty shall not normally be assigned to duties other than traffic enforcement, traffic accident prevention and investigation, escort duty, parade duty, and training.
 - (a) An exception may be made in order to assist in other police related duties as assigned and authorized by the Department.
 - (b) The officer shall operate the motorcycle throughout his/her assigned shift. The officer may operate a police automobile as an *exception* for any of the following reasons:
 - (a) Inclement weather such as dense fog, rain, snow, or on snow or ice covered road surfaces.
 - (b) Mental or physical condition of the officer.
 - (c) Motorcycle inoperative.
 - (d) Special assignment.
 - (e) Obvious emergency.
- (c) Assignment Criteria:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Motorcycle Officer Program

- (a) The assignment of motorcycle duty shall be restricted to the officers and Sergeant of the Motor Unit.
- (b) In addition, officers assigned to motorcycle duty must be certified as a Level 1 or 2 riders.
- (c) Motorcycles should not be used for a long-term pursuit. Use discretion at all times and pursue at Sergeant's discretion.
- (d) Motorcycles should not be used for specific duties such as warrant service, road blocks, or other tasks that do not require the special application of a motorcycle, and that expose the motor officer to more than reasonable risk.

507.1.2 SELECTION AND TRAINING

(a) Selection of Officers:

1. Police officers requesting the position of motorcycle operator within the Motor Unit must submit a letter of interest through the chain of command including the Motor Sergeant.
2. Notification of the next certification-training program will be sent to the officer.
3. The officer must obtain a valid Utah Motorcycle Operators License prior to any motorcycle training.
4. The officer is required to attend and successfully complete the initial certification program as designated by the South Salt Lake Police Department.
5. Upon successful completion of the training program, the officer will be considered a Level 2 Motor Officer.
6. The Traffic Unit Commander in cooperation with the Motor Sergeant will select Level 1 officers from the Level 2 certified officers. Once the officer is selected and transferred to the Motor Unit, the certification status will be upgraded to Level 1.
7. Level 1 riders transferred to the Motor Division will be placed on a six (6) month probation.
8. Selected officers are expected to comply with all orders, commands, signals and gestures of the Motor Training Instructor.
 - (a) Failure to comply may result in elimination from the motorcycle training program.

(b) Transfer or Rejection of Officers through Training:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Motorcycle Officer Program

- (a) When an officer fails to successfully complete the motorcycle certification program, an evaluation and reason for non-certification will be presented to the Motor Sergeant by the Motor Training Officer.
- (b) The officer will not be allowed to operate a motorcycle in any capacity other than supervised training until he/she successfully completes the certification program.
- (c) Certified officers (Level 1 and 2) must successfully complete a re-certification once a year.
 - (a) If a Level 1 or 2 officers fails to complete a re-certification, he/she must successfully complete the re-certification training within 45 days.
 - (b) The training officer will re-schedule a re-certification within the 45-day period.
 - (c) If the Level 1 or 2 officers fails to complete the second re-certification training, that officer will be relieved of motorcycle duty and transferred out of the Motor Unit.
- (c) Motorcycle Enforcement Training:
 - 1. Officers are required to pass the Utah Highway Patrol Basic Police Motorcycle Skills Course before being placed as a Level 1 or Level 2 rider.
 - 2. The records of motorcycle training for each officer in the Motor Unit shall be kept and updated by the Motor Training Instructor and Motor Sergeant.
 - 3. The training records shall be open for review by the officer, administrative officers, and the Motor Training Instructor.
 - 4. Motor Training Instructors shall conduct the initial certification and re-certification of police officers. Only Motor Training Instructors are responsible for trainee evaluations during and following the training program.
- (d) Motorcycle Enforcement Instructors:
 - 1. Officers must obtain a current motorcycle instructor certificate, or other qualified instructor certificate recognized by the Chief of Police and P.O.S.T. to be considered a Motorcycle-Training Instructor by this department.
 - 2. The department Motor Training Instructor(s) will be designated by the Motor Unit Sergeant and the Traffic Unit Commander.
 - 3. Only officers with 2 years or more at Level 1 status can be considered eligible for instructor.
 - (a) The Motor Training Instructor may select "Training Assistants" from Level 1 officers.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Motorcycle Officer Program

4. Motor Training Instructor must demonstrate the ability to train, counsel, and objectively evaluate a trainee.
5. Motor Training Instructor must maintain a positive attitude and demonstrate the desire and ability to meet departmental objectives.
6. Motor Training Instructor are responsible for:
 - (a) Ensuring the safety of the trainee.
 - (b) Fulfilling the purposes of the program.
 - (c) Providing constructive criticism and necessary counseling for the trainees.
 - (d) Emphasizing the development and maintenance of riding skills and safety consciousness.
 - (e) Informing supervisors of any potential safety risk surrounding any motorcycle officer or trainee.
 - (f) Developing officers who are effective in their motorcycle patrol and enforcement techniques.
 - (g) Introducing the trainee to a variety of riding conditions commensurate with the trainee's progressive ability.
 - (h) Eliminating riders who fail to develop the proper skills and outlook necessary to safely perform the duties of an enforcement rider.
7. The designated Motor Training Instructor must maintain an updated training file on every officer involved in the program. The file will include the following:
 - (a) Time spent on each area of instruction and practical application.
 - (b) Any areas of proficiency deficits and a plan for improvement.
 - (c) Any reports of collisions or neglect/misuse of equipment.
 - (d) Officer attitude and recommendations as it relates to training or riding ability.
8. The Motor Training Instructor shall present a written lesson plan for each phase of initial certification and re-certification to the Motor Sergeant and the department Training Supervisor no later than 14 days prior to the scheduled training day(s).
 - (a) The lesson plan may also be subject to review by the department administration, or any agent of the City, as designated by the Chief of Police.
 - (b) The Chief of Police may reject all or any part of the lesson plan if found to be without merit or presents a risk of liability to the City or its agents.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Motorcycle Officer Program

- (c) The lesson plan for each phase of training shall be retained by the Motor Training Instructor for a minimum of three (3) years.

507.1.3 MOTORCYCLE COLLISIONS INVOLVING DEPARTMENT-ISSUED EQUIPMENT

A motorcycle collision, not related to supervised training, as it applies to policy shall include but not be limited to the following criteria:

- (a) The motorcycle sustains damage due to a collision of any kind.
- (b) The motorcycle rider or anyone is injured, however slight, by the operation or malfunction of a department motorcycle.
- (c) The motorcycle collision shall be reported in accordance with the standard departmental vehicle collision report criteria (Policy 502).
- (d) Any collision or damage to the motorcycle, including incidents related to training, shall be reported in writing to the Motor Sergeant.
 - 1. The written report shall be placed in the motor training file and in the file of the officer involved.

507.1.4 EQUIPMENT AND MAINTENANCE

Equipment installed at the direction of or by the motorcycle manufacturer is standard. Minor changes, alterations or addition of equipment may be permitted at the discretion of Motor Sergeant, in cooperation with the Motor Training Instructor and a qualified police motorcycle service agent or representative, and adhere to the following:

- (a) Any change, alteration, or addition of equipment shall be consistent on all motorcycles in the Motor Unit.
- (b) Any change, alteration, or addition of equipment, shall be approved by the Traffic Unit Commander.
- (c) Replacement of department motorcycles should take place at the recommendation of the Motor Sergeant, the administration and fleet manager.
- (d) The purchase of new or used motorcycles and/or equipment should be done with input from the Motor Sergeant.

507.1.5 MOTORCYCLE SECURITY AND INSPECTIONS

- (a) All motorcycles used by Level 1 officers shall be inspected daily by the assigned motor officer.
- (b) All motor officers should inspect their assigned motorcycles before or at the beginning of each shift.
- (c) At least once a month, the Motor Sergeant should accompany motor officers during an inspection of their assigned motorcycles.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Motorcycle Officer Program

- (d) Mechanical problems discovered during any inspection shall be reported immediately to the Motor Sergeant. The Motor Sergeant will determine if the motorcycle needs to take out-of-service for repair.
- (e) When stored at a location other than a department facility, motorcycles shall be under cover in an enclosed area. A carport does not meet this requirement.

507.1.6 TRAFFIC STOPS

Officer safety is always the first priority.

- (a) Try to stop the violator where there is sufficient room on the right edge of the roadway or solid road shoulder to avoid exposure to other traffic.
- (b) Do not stop in front of violator's vehicle. If you are forced to pass during the stop, circle back and re-position prior to dismounting the motorcycle.
- (c) Dismount the motorcycle on the right side.
- (d) If traffic conditions, speed, visibility, or any other impairment restricts the normal safety expectations of the rider, use good judgment and reconsider the stop.
- (e) High Risk Stops:
 - 1. Assistance should be present prior to making the stop if at all possible. A motor officer is at a definite disadvantage. An automobile unit should be present.
 - 2. Do not park as close to the rear of the suspect vehicle as you would on other violator stops.
 - 3. Park in a diagonal position as this may provide some protection.
 - 4. Use telephone poles, mailboxes, parked cars, etc., for additional protection.
 - 5. Determine if you can handle your weapon(s) with your gloves on. If not, develop a technique to remove them prior to making the stop.

507.1.7 RIDING AT NIGHT

Officers riding motorcycles after dark should, when possible, pair up with another motor officer throughout the tour of duty. This will increase the visibility of the motor officers to the other drivers on the road. In case of a collision in a dark location, the partner will be there to offer assistance.

507.1.8 MOTOR OFFICER PARTNER ASSIGNMENT

All officers riding motorcycles should be assigned a partner within the Motor Unit, with the exception of the Sergeant or when on special assignment. Officers should retain the same partners for a minimum of 3 consecutive months. This is considered a safety issue. Officers need time to adapt to the other officer's riding style.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Motorcycle Officer Program

507.1.9 FORMATION AND ESCORT RIDING

When assigned to escort a group such as runners, walking groups, bicyclists, youth parades, etc., the following procedures apply:

- (a) The Motor Sergeant or senior riding Level 1 officer should assume the front left position to lead the procession, with one officer on the right.
- (b) Two motor officers should pair-up to lead processions. Two additional motor officers should pair-up and control the middle portion of the group.
- (c) One or more officers should follow the procession or group.
- (d) Assistance of patrol cars may be required to control intersections.

507.1.10 ESCORT REQUESTS AND COORDINATION

The Motor Sergeant shall coordinate all requests for escort participation.

- (a) Funeral Escorts:
 - 1. Two officers should lead the procession to control major intersections.
 - 2. Once the intersection is controlled, one officer should proceed to the next intersection.
 - (a) These officers may alternate positions.
 - 3. One officer should take a position at the left front side of the hearse throughout the procession.
 - 4. One officer should follow the last vehicle in the procession and be available to assist in intersection control.
 - 5. Assistance of patrol cars may be required to control intersections.
 - 6. If the Motor Unit is assisting another police agency, that agency may make position assignments.
- (b) Parade Routines and Escort:
 - (a) The Motor Sergeant will plan and direct all formations, positions, and assignments for parade participation.
 - (b) The Motor Sergeant will coordinate details of the parade position and participation with the parade committee or group.

Chapter 6 - Investigation Operations

Investigation and Prosecution

600.1 PURPOSE AND SCOPE

The purpose of this policy is to set guidelines and requirements pertaining to the handling and disposition of criminal investigations.

600.1.1 POLICY

Whether talking with a witness, or a suspect in a case under investigation, employees of the South Salt Lake City Police Department will conduct themselves in a professional and ethical manner. Interviews and interrogations will be conducted within the framework of state and federal guidelines and show regard for basic human decency and dignity.

With regard to exculpatory evidence, investigations must be conducted in a non-bias manner. During the course of an investigation, from initial call to the completion of the investigation and beyond; that all evidence, regardless of whether it supports the prosecution or the defense, must be documented and relinquished in the discovery process. This is based on two cases: *Brady v. Maryland*, 373 U.S. 83 (1963); and *Giglio V. United States*, 450 U.S. 150 (1972).

600.2 POLICY

It is the policy of the South Salt Lake Police Department to investigate crimes thoroughly and with due diligence, and to evaluate and prepare criminal cases for appropriate clearance or submission to a prosecutor.

600.3 INITIAL INVESTIGATION

600.3.1 OFFICER RESPONSIBILITIES

An officer responsible for an initial investigation shall complete no less than the following:

- (a) Make a preliminary determination of whether a crime has been committed by completing, at a minimum:
 - 1. An initial statement from any witnesses or complainants.
 - 2. A cursory examination for evidence.
- (b) If information indicates a crime has occurred, the officer shall:
 - 1. Preserve the scene and any evidence as required to complete the initial and follow-up investigation.
 - 2. Determine if additional investigative resources (e.g., investigators or scene processing) are necessary and request assistance as required.
 - 3. If assistance is warranted, or if the incident is not routine, notify a supervisor or the Watch Commander.
 - 4. Make reasonable attempts to locate, identify and interview all available victims, complainants, witnesses and suspects.
 - 5. Collect any evidence.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Investigation and Prosecution

6. Take any appropriate law enforcement action.
 7. Complete and submit the appropriate reports and documentation.
- (c) If the preliminary determination is that no crime occurred, determine what other action may be necessary, what other resources may be available, and advise the informant or complainant of this information.

600.3.2 NON-SWORN MEMBER RESPONSIBILITIES

A non-sworn member assigned to any preliminary investigation is responsible for all investigative steps, except making any attempt to locate, contact or interview a suspect face-to-face or take any enforcement action. Should an initial investigation indicate that those steps are required, the assistance of an officer shall be requested.

600.3.3 CRIME SCENE PROCESSING

The [Department/Office] has access to crime scene investigators on a 24-hour basis to process crime scenes. The Watch Commander or the authorized designee shall notify the appropriate members or agency when investigative or processing assistance is needed.

600.4 CUSTODIAL INTERROGATION REQUIREMENTS

Suspects who are in custody and subjected to an interrogation shall be given the *Miranda* warning, unless an exception applies. Interview or interrogation of a juvenile shall be in accordance with the Temporary Custody of Juveniles Policy.

600.4.1 AUDIO/VIDEO RECORDINGS

Any custodial interrogation of an individual who is suspected of having committed any violent felony offense as defined in Utah Code 76-3-203.5(1)(c)(i) should be recorded (audio or video with audio as available) in its entirety. Regardless of where the interrogation occurs, every reasonable effort should be made to secure functional recording equipment to accomplish such recordings.

Consideration should also be given to recording a custodial interrogation, or any investigative interview, for any other offense when it is reasonable to believe it would be appropriate and beneficial to the investigation and is otherwise allowed by law.

No recording of a custodial interrogation should be destroyed or altered without written authorization from the prosecuting attorney and the Investigations Division supervisor. Copies of recorded interrogations or interviews may be made in the same or a different format as the original recording, provided the copies are true, accurate and complete and are made only for authorized and legitimate law enforcement purposes.

Recordings should not take the place of a thorough report and investigative interviews. Written statements from suspects should continue to be obtained when applicable.

The guidelines for recording a custodial interrogation are not applicable if:

- (a) The suspect refuses to speak if the interrogation is electronically recorded. Any such refusal should be documented either by audio/video recording demonstrating such refusal, or through a written statement signed by the suspect.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Investigation and Prosecution

- (b) Despite the reasonable good faith efforts of the officer to obtain or provide recording equipment, recording equipment is not reasonably available during the period of time that the suspect is lawfully detained.
- (c) The recording equipment malfunctions and replacement equipment is not reasonably available.
- (d) Despite the reasonable good faith efforts of the officer to record the interrogation, the recording equipment, without the officer's knowledge, malfunctions or stops operating.
- (e) The officer conducting the custodial interrogation reasonably believes that the crime of which the person is suspected of committing is not a violent felony offense.
- (f) Exigent circumstances render electronic recording impossible or impracticable.

600.5 DISCONTINUATION OF INVESTIGATIONS

The investigation of a criminal case or efforts to seek prosecution should only be discontinued if one of the following applies:

- (a) All reasonable investigative efforts have been exhausted, no reasonable belief that the person who committed the crime can be identified, and the incident has been documented appropriately.
- (b) The perpetrator of a misdemeanor has been identified and a warning is the most appropriate disposition.
 - 1. In these cases, the investigator shall document that the person was warned and why prosecution was not sought.
 - 2. Warnings shall not be given for felony offenses or other offenses identified in this policy or by law that require an arrest or submission of a case to a prosecutor.
- (c) The case has been submitted to the appropriate prosecutor but no charges have been filed. Further investigation is not reasonable nor has the prosecutor requested further investigation.
- (d) The case has been submitted to the appropriate prosecutor, charges have been filed, and further investigation is not reasonable, warranted or requested, and there is no need to take the suspect into custody.
- (e) Suspects have been arrested, there are no other suspects, and further investigation is either not warranted or requested.
- (f) Investigation has proven that a crime was not committed (see the Sexual Assault Investigations Policy for special considerations in these cases).

The Domestic Violence, Child Abuse, Sexual Assault Investigations and Adult Abuse policies may also require an arrest or submittal of a case to a prosecutor.

600.6 COMPUTERS AND DIGITAL EVIDENCE

The collection, preservation, transportation and storage of computers, cell phones and other digital devices may require specialized handling to preserve the value of the related evidence. If it is anticipated that computers or similar equipment will be seized, officers should request that

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Investigation and Prosecution

computer forensic examiners assist with seizing computers and related evidence. If a forensic examiner is unavailable, officers should take reasonable steps to prepare for such seizure and use the resources that are available.

600.7 INVESTIGATIVE USE OF SOCIAL MEDIA AND INTERNET SOURCES

Use of social media and any other internet source to access information for the purpose of criminal investigation shall comply with applicable laws and policies regarding privacy, civil rights, and civil liberties. Information gathered via the internet should only be accessed by members while on-duty and for purposes related to the mission of this [department/office]. If a member encounters information relevant to a criminal investigation while off-duty or while using the member's own equipment, the member should note the dates, times, and locations of the information and report the discovery to the member's supervisor as soon as practicable. The member, or others who have been assigned to do so, should attempt to replicate the finding when on-duty and using [department/office] equipment.

Information obtained via the internet should not be archived or stored in any manner other than [department/office]-established record keeping systems (see the Records Maintenance and Release and Criminal Organizations policies).

600.7.1 ACCESS RESTRICTIONS

Information that can be accessed from any [department/office] computer, without the need of an account, password, email address, alias, or other identifier (unrestricted websites), may be accessed and used for legitimate investigative purposes without supervisory approval.

Accessing information from any internet source that requires the use or creation of an account, password, email address, alias, or other identifier, or the use of nongovernment IP addresses, requires supervisor approval prior to access. The supervisor will review the justification for accessing the information and consult with legal counsel as necessary to identify any policy or legal restrictions. Any such access and the supervisor approval shall be documented in the related investigative report.

Accessing information that requires the use of a third party's account or online identifier requires supervisor approval and the consent of the third party. The consent must be voluntary and shall be documented in the related investigative report.

Information gathered from any internet source should be evaluated for its validity, authenticity, accuracy, and reliability. Corroborative evidence should be sought and documented in the related investigative report.

Any information collected in furtherance of an investigation through an internet source should be documented in the related report. Documentation should include the source of information and the dates and times that the information was gathered.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Investigation and Prosecution

600.7.2 INTERCEPTING ELECTRONIC COMMUNICATION

Intercepting social media communications in real time may be subject to federal and state wiretap laws. Officers should seek legal counsel before any such interception.

600.8 MODIFICATION OF CHARGES FILED

Members are not authorized to recommend to the prosecutor or to any other official of the court that charges on a pending case be amended or dismissed without the authorization of a Division Commander or the Chief of Police. Any authorized request to modify the charges or to recommend dismissal of charges shall be made to the prosecutor.

600.9 IDENTITY THEFT

A report should be taken any time a person living within the jurisdiction of the [Department/Office] reports that the person has been a victim of identity theft. This includes:

- (a) Taking a report, even if the location of the crime is outside the jurisdiction of this [department/office] or has not been determined.
- (b) Providing the victim with the appropriate information, as set forth in the Victim and Witness Assistance Policy. [Department/Office] members should encourage the individual to review the material and should assist with any questions.

A report should also be taken if a person living outside [department/office] jurisdiction reports an identity theft that may have been committed or facilitated within this jurisdiction (e.g., use of a post office box in South Salt Lake to facilitate the crime).

A member investigating a case of identity theft should ensure that the case is referred to the appropriate agency if it is determined that this [department/office] should not be the investigating agency (e.g., an identity theft ring working from out of state). The victim should be advised that the case is being transferred to the agency of jurisdiction. The appropriate entries should be made into any databases that have been authorized for [department/office] use and are specific to this type of investigation.

Detective Availability

601.1 PURPOSE AND SCOPE

In order to provide 24- hour detective coverage, an "on-call" schedule of detectives will be established and maintained by the Investigation Section Sergeant.

- (a) The Investigation Section Sergeant will ensure that the communications center, patrol division sergeants and the Investigations Division Commander are notified of a detective's status by means of an on-call roster.
- (b) Detectives who are not on-call are not required to be available to the department via their Department cell phones at all times.
 - 1. In the event of a "major case" that would require more than one detective, additional detectives will be called out.
 - 2. Detectives are paid additional money over their base salary for being on-call for these events.
 - 3. It is imperative that the Investigation Section Sergeant be kept informed of a detective's availability. The following is required of all detectives who are not in on-call status:
 - (a) Notify the Detective Sergeant whenever they will be unavailable for call-outs.
 - (b) Carry their department cell phones with them at all times when available for call-outs.
- (c) It is important for the detective section of the police department be prepared and able to adequately and promptly respond to "major case" events.
- (d) Detectives who fail to meet the needs of the department may be subject to removal from the detective section and/or disciplinary action.

Sexual Assault Investigations

602.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the investigation of sexual assaults (Utah Code 53-25-201). These guidelines will address some of the unique aspects of such cases and the effects that these crimes have on the victims.

Mandatory notifications requirements are addressed in the Child Abuse and Adult Abuse policies.

602.1.1 DEFINITIONS

Definitions related to this policy include:

Restricted sexual assault kit - A sexual assault kit collected from a victim who is at least 18 years old and at the time of collection declines to have the kit processed or to have the examination form shared with any entity outside of the collection facility (Utah Code 53-10-902).

Sexual assault - Any crime or attempted crime of a sexual nature, to include but not limited to offenses defined in Utah Code, Title 76, Chapter 5, Part 4 (Sexual Offenses).

Sexual assault kit - A package of items that is used by medical personnel to gather and preserve biological and physical evidence following an allegation of a sexual offense (Utah Code 53-10-902).

Sexual Assault Response Team (SART) - A multidisciplinary team generally comprised of advocates; law enforcement officers; forensic medical examiners, including sexual assault forensic examiners (SAFEs) or sexual assault nurse examiners (SANEs) if possible; forensic laboratory personnel and prosecutors. The team is designed to coordinate a broad response to sexual assault victims.

602.2 POLICY

It is the policy of the South Salt Lake Police Department that its members, when responding to reports of sexual assaults, will strive to minimize the trauma experienced by the victims, and will aggressively investigate sexual assaults, pursue expeditious apprehension and conviction of perpetrators, and protect the safety of the victims and the community.

602.3 QUALIFIED INVESTIGATORS

Qualified investigators should be available for assignment of sexual assault investigations. These investigators should:

- (a) Have specialized training in, and be familiar with, interview techniques and the medical and legal issues that are specific to sexual assault investigations.
- (b) Conduct follow-up interviews and investigation.
- (c) Present appropriate cases of alleged sexual assault to the prosecutor for review.
- (d) Coordinate with other enforcement agencies, social service agencies and medical personnel as needed.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Sexual Assault Investigations

- (e) Provide referrals to therapy services, victim advocates and support for the victim.
- (f) Participate in or coordinate with the SART or other multidisciplinary investigative teams as applicable.

602.4 REPORTING

In all reported or suspected cases of sexual assault, a report should be written and assigned for follow-up investigation. This includes incidents in which the allegations appear unfounded or unsubstantiated.

602.5 VICTIM INTERVIEWS

The primary considerations in sexual assault investigations, which begin with the initial call to Dispatch, should be the health and safety of the victim, the preservation of evidence, and preliminary interviews to determine if a crime has been committed and to attempt to identify the suspect.

Whenever possible, a member of the SART should be included in the initial victim interviews.

An in-depth follow-up interview should not be conducted until after the medical and forensic examinations are completed and the personal needs of the victim have been met (e.g., change of clothes, bathing). The follow-up interview may be delayed to coordinate with victim based upon the circumstances. Whenever practicable, the follow-up interview should be conducted by a qualified investigator.

No opinion of whether the case is unfounded should be included in a report.

Victims should not be asked or required to take a polygraph examination (34 USC § 10451).

Victims should be apprised of applicable victim's rights provisions, as outlined in the Victim and Witness Assistance Policy.

602.5.1 MEMBER RESPONSIBILITIES

A victim, or victim's designee, should be informed of applicable victim's rights, including the rights for victims of sexual offenses (Utah Code 77-37-3). Investigating members shall, in a timely manner, provide the victim or the victim's designee with the information required by Utah Code 77-37-3 (e.g., DNA profile obtained, CODIS matches), including, if requested, any significant changes in the information.

602.5.2 NOTIFICATION UPON ARREST OR ISSUANCE OF A CITATION

When an officer arrests or issues a citation to a person 18 years of age or older for a qualifying sexual offense, the officer shall provide the individual with the written notice required by Utah Code 78B-7-802. Victims shall be provided notice in accordance with the Victim and Witness Assistance Policy.

602.6 COLLECTION AND TESTING OF BIOLOGICAL EVIDENCE

Whenever possible, a SART member should be involved in the collection of forensic evidence from the victim.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Sexual Assault Investigations

When the facts of the case indicate that collection of biological evidence is warranted, it should be collected regardless of how much time has elapsed since the reported assault.

If a drug-facilitated sexual assault is suspected, urine and blood samples should be collected from the victim as soon as practicable.

Subject to the requirements set forth in this policy, biological evidence from all sexual assault cases, including cases where the suspect is known by the victim, should be submitted for testing.

Victims who choose not to assist with an investigation, do not desire that the matter be investigated or wish to remain anonymous may still consent to the collection of evidence under their control. In these circumstances, the evidence should be collected and stored appropriately.

602.6.1 COLLECTION AND TESTING REQUIREMENTS

Members investigating sexual assaults or handling related evidence are required to:

- (a) Notify the victim, or his/her designee, if evidence will not be analyzed in a case involving an unknown perpetrator (Utah Code 77-37-3).
- (b) Take possession of sexual assault kits within one business day after receiving notice from a collecting facility (Utah Code 76-5-604; Utah Code 76-5-607).
 - 1. The member taking possession of the kit should ensure that the required information is entered into the statewide sexual assault kit tracking system within five days of receiving the kit from a collection facility.
- (c) Transfer the kit to the appropriate law enforcement agency within 10 days in cases where the incident occurred in another jurisdiction (Utah Code 76-5-604).
- (d) Submit the kit to the Utah Bureau of Forensic Services within 30 days of obtaining possession of the kit except for cases involving restricted kits (Utah Code 76-5-604).
 - 1. If available, a suspect standard or a consensual partner elimination standard shall be submitted with the sexual assault kit.
 - 2. If not obtained until later, the standards shall be submitted as soon as possible but no later than 30 days after the department obtained possession of the kit.
 - 3. If the victim at any time chooses to provide a statement about the incident to law enforcement, the kit shall no longer be classified as restricted and shall be submitted to the Utah Bureau of Forensic services as soon as possible, but no later than 30 days after the victim provides the statement (Utah Code 76-5-604).

Additional guidance regarding evidence retention and destruction is found in the Property and Evidence Policy.

602.6.2 DNA TEST RESULTS

Members investigating sexual assault cases should ensure that a victim, or their designee, is notified of any DNA test results as soon as reasonably practicable (Utah Code 77-37-3).

A SART member should be consulted regarding the best way to deliver biological testing results to a victim so as to minimize victim trauma, especially in cases where there has been a significant

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Sexual Assault Investigations

delay in getting biological testing results (e.g., delays in testing the evidence or delayed DNA databank hits). Members should make reasonable efforts to assist the victim by providing available information on local assistance programs and organizations as provided in the Victim and Witness Assistance Policy.

Members investigating sexual assaults cases should ensure that DNA results are entered into databases when appropriate and as soon as practicable.

602.6.3 COLLECTION AND TESTING REQUIREMENTS

Members investigating sexual assaults or handling related evidence are required to:

- (a) Notify the victim, or the victim's designee, if evidence will not be analyzed in a case involving an unknown perpetrator (Utah Code 77-37-3).
- (b) Take possession of sexual assault kits within one business day after receiving notice from a collecting facility (Utah Code 53-10-904; Utah Code 53-10-907).
 - 1. The member taking possession of the kit should ensure that the required information is entered into the statewide sexual assault kit tracking system within five days of receiving the kit from a collection facility.
- (c) Transfer the kit to the appropriate law enforcement agency within 10 days in cases where the incident occurred in another jurisdiction (Utah Code 53-10-904).
- (d) Submit the kit to the Utah Bureau of Forensic Services within 30 days of obtaining possession of the kit except for cases involving restricted kits (Utah Code 53-10-904).
 - 1. If available, a suspect standard or a consensual partner elimination standard shall be submitted with the sexual assault kit.
 - 2. If not obtained until later, the standards shall be submitted as soon as possible but no later than 30 days after the [Department/Office] obtained possession of the kit.
 - 3. If the victim informs the South Salt Lake Police Department that the victim wants to have the kit processed and agrees to release of the sexual assault examination form with the kit, the kit may no longer be classified as restricted and shall be submitted to the Utah Bureau of Forensic Services as soon as possible, but no later than 30 days after the victim chooses to unrestrict the kit (Utah Code 53-10-904).

Additional guidance regarding evidence retention and destruction is found in the Property and Evidence Policy.

602.7 DISPOSITION OF CASES

If the assigned investigator has reason to believe the case is without merit, the case may be classified as unfounded only upon review and approval of the Investigations Division supervisor.

Classification of a sexual assault case as unfounded requires the Investigations Division supervisor to determine that the facts have significant irregularities with reported information and that the incident could not have happened as it was reported. When a victim has recanted his/

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Sexual Assault Investigations

her original statement, there must be corroborating evidence that the allegations were false or baseless (i.e., no crime occurred) before the case should be determined as unfounded.

602.8 CASE REVIEW

The Investigations Division supervisor should ensure cases are reviewed on a periodic basis, at least annually, using an identified group that is independent of the investigation process. The reviews should include an analysis of:

- Case dispositions.
- Decisions to collect biological evidence.
- Submissions of biological evidence for lab testing.

The SART and/or victim advocates should be considered for involvement in this audit. Summary reports on these reviews should be forwarded through the chain of command to the Chief of Police.

602.9 RELEASING INFORMATION TO THE PUBLIC

In cases where the perpetrator is not known to the victim, and especially if there are multiple crimes where more than one appear to be related, consideration should be given to releasing information to the public whenever there is a reasonable likelihood that doing so may result in developing helpful investigative leads. The Investigations Division supervisor should weigh the risk of alerting the suspect to the investigation with the need to protect the victim and the public, and to prevent more crimes.

602.10 TRAINING

Subject to available resources, periodic training should be provided to:

- (a) Members who are first responders. Training should include:
 1. Initial response to sexual assaults.
 2. Legal issues.
 3. Victim advocacy.
 4. Victim's response to trauma.
- (b) Qualified investigators, who should receive advanced training on additional topics. Advanced training should include:
 1. Interviewing sexual assault victims.
 2. SART.
 3. Medical and legal aspects of sexual assault investigations.
 4. Serial crimes investigations.
 5. Use of community and other federal and state investigative resources, such as the Violent Criminal Apprehension Program (ViCAP).
 6. Techniques for communicating with victims to minimize trauma.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Sexual Assault Investigations

602.11 PUBLIC ACCESS

This policy shall be published on the [Department/Office] website for public access (Utah Code 53-25-201).

Asset Forfeiture

603.1 PURPOSE AND SCOPE

This policy describes the authority and procedure for the seizure, forfeiture and liquidation of property associated with specified designated offenses.

603.1.1 DEFINITIONS

Definitions related to this policy include:

Contraband - Any item that is unlawful to produce or possess under state or federal law, including controlled substances possessed, transferred, or distributed in violation of the Utah Controlled Substances Act and computers used to commit crimes involving child sexual abuse material or identity theft (Utah Code 77-11a-101).

Forfeiture - The process by which legal ownership of an asset is transferred to a government or other authority.

Forfeiture reviewer - The [department/office] member assigned by the Chief of Police who is responsible for reviewing all forfeiture cases and for acting as the liaison between the [Department/Office] and the assigned attorney.

Property subject to forfeiture - Seized property that has been used to facilitate the commission of a federal or state offense and seized proceeds when authorized under Utah Code 77-11b-102 (Utah Code 77-11a-101).

Seizure - The act of law enforcement officials taking property, cash, or assets that have been used in connection with or acquired by specified illegal activities.

603.1.2 POLICY

It shall be the policy of the South Salt Lake City Police Department to pursue the forfeiture of any assets that are the proceeds of a criminal act, or were used to facilitate a criminal act. Assets used to "facilitate a criminal act" is typically associated with economic crimes, investment scams, property offenses and controlled substances violations, and is pursuant to State or Federal laws.

The Department shall designate at least one sworn officer as the Asset Forfeiture Officer (AFO) who will be the liaison with the prosecutor assigned to forfeiture cases. The AFO is responsible for ensuring that Department forfeitures adhere to state and federal law. The AFO will adhere to unit procedures relating to forfeiture, ensuring forfeiture actions are in proportion to the violation or crime committed.

603.1.3 PROCEDURES FOR FORFEITURE OF ASSETS UNDER STATE LAW

The procedure for the forfeiture of assets is regulated by State Code Annotated § 24-1-2. Some sections of the law also provide specific information about when, and how, assets can be seized for forfeiture. (See Utah Code Annotated 58-37-13, Controlled Substances Act)

- (a) Field Unit Procedures:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Asset Forfeiture

1. Whenever reporting officers identify assets that may be subject to potential forfeiture under state law, they shall notify a supervisor and advise the supervisor of the following:
 - (a) Circumstances that resulted in the officer discovering the asset(s).
 - (b) Description of the asset(s).
 - (c) Reasons that the officer believes the asset(s) is forfeitable under state law.
 - (d) Receive permission from supervisor to seize the asset.
 - (e) Property that will not be seized includes:
 1. Property from innocent owners.
 2. Property that contains only a trace amount of a controlled substance.
 3. Any time the seizure of the asset(s) is not in the interests of the state.
 - (f) Interview the person in custody of the asset(s) to determine if the asset(s) were proceeds of a criminal act, or were used to facilitate a criminal act.
 - (g) Complete the "South Salt Lake City Police Department ASSET SEIZURE NOTIFICATION FORM" and provide a copy to the person who is in custody of the asset(s). If no person is present, leave a copy in a conspicuous place.
 - (h) Document the circumstances in a report and provide specific information about why the asset(s) is/are believed to be proceeds of illegal activity or have facilitated an illegal activity.
 1. Provide notice of the forfeiture to the AFO/detective sergeant. This notice may be given by phone or electronically.
 - (i) Follow Department procedures for the proper booking of the asset(s) in evidence.
- (b) Investigations Unit Procedures:
 1. Detectives shall bring any case that has the potential for asset forfeiture to the attention of the AFO who shall:
 - (a) Review the circumstances of the case to determine if any asset has the potential to be seized under State or Federal law.
 - (b) If so, begin the asset forfeiture process.
 - (c) The AFO will deal ONLY with the asset forfeiture portion of the case, and will not investigate any other portion of the case.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Asset Forfeiture

2. If, during the normal course of duty, an investigator locates and identifies property that may be subject to possible forfeiture, the investigator shall follow the procedures in section A above, as outlined for Field Units.

603.2 POLICY

The South Salt Lake Police Department recognizes that appropriately applied forfeiture laws are helpful to enforce the law, deter crime and reduce the economic incentive of crime. However, the potential for revenue should never compromise the effective investigation of criminal offenses, officer safety or any person's due process rights.

It is the policy of the South Salt Lake Police Department that all members, including those assigned to internal or external law enforcement task force operations, shall comply with all state and federal laws pertaining to forfeiture.

603.2.1 IMPOUNDING A VEHICLE SEIZED FOR ASSET FORFEITURE

- (a) A vehicle will only be seized after the AFO has been notified and has given authorization.
- (b) Any vehicle that is identified as being possible profits of a criminal activity shall be impounded, marked as a "hold for investigation impound" per departmental policy and procedures.
 1. The vehicle should be held within the locked, gated, parking area of the South Salt Lake City Public Works for the appropriate detective unit.
- (c) The following will be documented in the report:
 1. Any lien-holder or other person/entity that may have an interest in the vehicle.
 2. Whether or not the registered owner was the driver or a passenger in the vehicle.
 3. Any information that reveals that the owner or interest holder had knowledge of the activity that subjected the vehicle to seizure.
 4. If the seizure is associated with a narcotics case, include the type and weight of the narcotics found.

603.3 ASSET SEIZURE

Property and contraband may be seized for forfeiture as provided in this policy.

603.3.1 PROPERTY AND CONTRABAND SUBJECT TO SEIZURE

- (a) Property and contraband that may be seized upon review and approval of a supervisor and in coordination with the forfeiture reviewer includes (Utah Code 77-11a-201):
 1. Property subject to forfeiture that has been identified in a court order or is the subject of a prior judgment.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Asset Forfeiture

2. Property and contraband subject to forfeiture that is seized upon the authority of a search or administrative warrant.
- (b) Property and contraband subject to forfeiture can be lawfully seized without a court order when the seizure is incident to arrest or when there is probable cause to believe:
 1. It is directly or indirectly dangerous to health or safety.
 2. It is evidence of an offense.
 3. It has been used or was intended to be used to commit an offense.
 4. It constitutes the proceeds of an offense.

Whenever practicable, obtaining a court order for seizure prior to making a seizure is the preferred method.

A large amount of money standing alone is insufficient to establish the probable cause required to make a seizure.

603.3.2 PROPERTY NOT SUBJECT TO SEIZURE

Property that should not be seized for forfeiture includes (Utah Code 77-11b-102):

- (a) Property that does not meet the forfeiture counsel's current minimum forfeiture guidelines.
- (b) A motor vehicle used in a violation of driving under the influence of alcohol and/or drugs (Utah Code 41-6a-502); driving with any measurable controlled substance in the body (Utah Code 41-6a-517); negligently operating a vehicle resulting in injury (Utah Code 76-5-102.1); automobile homicide (Utah Code 76-5-207); or a local DUI ordinance may not be forfeited unless any of the following apply:
 1. The operator of the vehicle has previously been convicted of a specified offense committed after May 12, 2009.
 2. The operator of the vehicle was driving on a denied, suspended, revoked, or disqualified license and the denial, suspension, revocation, or disqualification was imposed based upon specified violations.
- (c) Property used to facilitate specific crimes related to pornography or material harmful to children (Utah Code 76-5c-202; Utah Code 76-5c-204; Utah Code 76-5c-205; Utah Code 76-5c-305) if the seizure would constitute a prior restraint or interference with a person's rights under the First Amendment to the U.S. Constitution or the Utah Constitution.
- (d) Property seized incident to an arrest solely for possession of a controlled substance or controlled substance analog under Utah Code 58-37-8(2)(a)(i).
- (e) Firearms belonging to an individual charged with possessing a firearm in a secure area of an airport if the individual may otherwise lawfully possess the firearm (Utah Code 24-4-102).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Asset Forfeiture

603.4 PROCESSING SEIZED PROPERTY FOR FORFEITURE

When property subject to this policy is seized, the officer making the seizure should ensure compliance with the following (Utah Code 77-11a-203):

- (a) Complete the applicable seizure forms and present the appropriate copy to the person from whom the property is seized. If property is seized from more than one person, a separate copy must be provided to each person, specifying the items seized. When property is seized and no one claims an interest in the property, the officer must leave the copy in the place where the property was found, if it is reasonable to do so.
- (b) Complete and submit a report and original seizure forms within 24 hours of the seizure, if practicable.
- (c) Forward the original seizure forms and related reports to the forfeiture reviewer within two days of seizure.

The officer will book seized property as evidence with the notation in the comment section of the property form, "Seized Subject to Forfeiture." Property seized subject to forfeiture should be booked on a separate property form. No other evidence from the case should be booked on this form.

Photographs should be taken of items seized, particularly cash, jewelry, and other valuable items.

Officers who suspect property may be subject to seizure but are not able to seize the property (e.g., the property is located elsewhere, the whereabouts of the property is unknown, it is real estate, bank accounts, non-tangible assets) should document and forward the information in the appropriate report to the forfeiture reviewer.

603.5 MAINTAINING SEIZED PROPERTY

The Evidence Room supervisor is responsible for ensuring compliance with the following:

- (a) All property received for forfeiture is reasonably secured and properly stored to prevent waste and preserve its condition (Utah Code 77-11a-204).
- (b) All property received for forfeiture is checked to determine if the property has been stolen.
- (c) Cash and other negotiable instruments are deposited into a restricted interest-bearing account designated solely for property subject to forfeiture within 30 days of seizure (Utah Code 77-11a-204).
- (d) All property received for forfeiture is retained until forfeiture is finalized or the property is returned to the claimant or the person with an ownership interest.
- (e) Property received for forfeiture is not used by the [Department/Office] unless the forfeiture action has been completed.
- (f) Associated documentation complies with Utah Code 77-11a-203.

603.5.1 EXPENDITURE OF FUNDS FROM FORFEITED ASSETS

All assets that are forfeited shall be expended in accordance with State and Federal law.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Asset Forfeiture

603.5.2 RESTRICTIONS ON TRANSFER, SALE OR AUCTION

Any asset(s) seized and forfeited by this Department may not be transferred, sold, or auctioned to any member of the Department.

603.5.3 IDENTIFICATION AND TRACKING OF SEIZED PROPERTY

The Evidence Room technician shall identify and track all seized property in the same manner as booked evidence (see the Property and Evidence Policy).

603.6 FORFEITURE REVIEWER

The Chief of Police will appoint a forfeiture reviewer. Prior to assuming duties, or as soon as practicable thereafter, the forfeiture reviewer should attend a course approved by the [Department/Office] on asset forfeiture (Utah Code 77-11b-105).

The responsibilities of the forfeiture reviewer include:

- (a) Remaining familiar with forfeiture laws, and the forfeiture policies of the forfeiture counsel.
- (b) Serving as the liaison between the [Department/Office] and the forfeiture counsel and ensuring prompt legal review of all seizures.
- (c) Making reasonable efforts to obtain annual training that includes best practices in pursuing, seizing, and tracking forfeitures.
- (d) Deciding whether the forfeiture is more appropriately made under state or federal forfeiture laws (Utah Code 77-11a-205). The forfeiture reviewer should contact federal authorities when appropriate.
- (e) Ensuring that responsibilities are clearly established whenever multiple agencies are cooperating in a forfeiture case.
- (f) Ensuring that seizure forms are available and appropriate for [department/office] use. These should include notice forms, a receipt form, and a checklist that provides relevant guidance to officers. The forms should be available in languages appropriate for the region and should contain spaces for:
 - 1. Names and contact information for all relevant persons and law enforcement officers involved.
 - 2. Information as to how ownership or other property interests may have been determined (e.g., verbal claims of ownership, titles, public records).
 - 3. A space for the signature of the person from whom property is being seized.
 - 4. A tear-off portion or copy, which should be given to the person from whom property is being seized, that includes the legal authority for the seizure, information regarding the process to contest the seizure, and a detailed description of the items seized.
 - 5. Any other information that may be needed to comply with Utah Code 77-11a-203.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Asset Forfeiture

- (g) Ensuring that those who may be involved in asset forfeiture receive training in the proper use of the seizure forms and the forfeiture process. The training should be developed in consultation with the appropriate legal counsel and may be accomplished through traditional classroom education, electronic media, Daily Training Bulletins (DTBs), or General Orders. The training should cover this policy and address any relevant statutory changes and court decisions.
- (h) Reviewing each asset forfeiture case to ensure that:
 - 1. Written documentation of the seizure and the items seized is in the case file.
 - 2. Independent legal review of the circumstances and propriety of the seizure is made in a timely manner (Utah Code 77-11b-201).
 - 3. The notice of intent to seek forfeiture has been given in a timely manner to those who hold an interest in the seized property (Utah Code 77-11b-201).
 - (a) Prior to serving the notice, a search of public records shall be completed to identify the name and address of each interest holder of the property (Utah Code 77-11b-201).
 - 4. Property is promptly released to those entitled to its return (Utah Code 77-11a-301; Utah Code 77-11a-304; Utah Code 77-11b-203).
 - 5. All changes to forfeiture status are forwarded to any supervisor who initiates a forfeiture case.
 - 6. Any cash received is delivered to the Evidence Room supervisor to be deposited.
 - 7. Assistance with the resolution of ownership claims and the release of property to those entitled is provided.
 - 8. Current minimum forfeiture thresholds are communicated appropriately to officers.
 - 9. A copy of the property receipt is kept in the case file and, if the property is transferred to another agency, a copy of the receipt is provided along with the property (Utah Code 77-11a-203).
 - 10. Any records of a related interview of a child are retained pursuant to Utah Code 53-13-110.5.
 - 11. The request for a forfeiture action has been presented to the forfeiture attorney as provided in Utah Code 77-11b-201.
- (i) Ensuring that the [Department/Office] disposes of property as provided by law following any forfeiture (Utah Code 77-11b-401).
- (j) Ensuring this policy and any related policies are periodically reviewed and updated to reflect current federal and state statutes and case law.

Forfeiture proceeds should be maintained in a separate fund or account subject to appropriate accounting control, with regular reviews or audits of all deposits and expenditures.

Forfeiture reporting and expenditures should be completed in the manner prescribed by the law and City financial directives (Utah Code 77-11b-404).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Asset Forfeiture

A written plan should be available that enables the Chief of Police to address any extended absence of the forfeiture reviewer, thereby ensuring that contact information for other law enforcement officers and attorneys who may assist in these matters is available.

603.7 DISPOSITION OF FORFEITED PROPERTY

No property seized shall be transferred, sold, or auctioned to an employee of this [department/office] (Utah Code 77-11a-204).

No member of this [department/office] may use property that has been seized for forfeiture until the forfeiture action has been completed and the Chief of Police has given written authorization to retain the property for official use. No [department/office] member involved in the decision to seize property should be involved in any decision regarding the disposition of the property.

Any property, money, or other items of value received by this [department/office] pursuant to a federal forfeiture shall be used in compliance with federal laws and regulations relating to equitable sharing (Utah Code 77-11a-205). Such property may be used to fund crime prevention and law enforcement activities described in Utah Code 77-11b-403(10). State law prohibits the use of property or money received to be used for such things as salaries, benefits, any expenses not related to law enforcement, and other purposes specified in Utah Code 77-11b-403(11).

Money received as a result of a federal forfeiture may only be used as approved by the City council (Utah Code 77-11a-205).

603.8 LIMITATION ON FEES FOR HOLDING SEIZED PROPERTY

The [Department/Office] will not charge a person contesting a forfeiture any fee or cost for holding seized property as the result of any civil or criminal forfeiture in which a judgment is entered in favor of the person, or where a forfeiture proceeding is voluntarily dismissed by the prosecuting attorney (Utah Code 77-11b-306).

Informants

604.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the use of informants.

604.1.1 DEFINITIONS

Definitions related to this policy include:

Informant - A person who covertly interacts with other individuals or suspects at the direction of, request of, or by agreement with the South Salt Lake Police Department for law enforcement purposes. This also includes a person agreeing to supply information to the South Salt Lake Police Department for a benefit (e.g., a quid pro quo in the form of a reduced criminal penalty, money).

604.2 POLICY

The South Salt Lake Police Department recognizes the value of informants to law enforcement efforts and will strive to protect the integrity of the informant process. It is the policy of this department that all funds related to informant payments will be routinely audited and that payments to informants will be made according to the criteria outlined in this policy.

604.3 USE OF INFORMANTS

604.3.1 INITIAL APPROVAL

Before using an individual as an informant, an officer must receive approval from his/her supervisor. The officer shall compile sufficient information through a background investigation and experience with the informant in order to determine the suitability of the individual, including age, maturity and risk of physical harm, as well as any indicators of his/her reliability and credibility.

Members of this department should not guarantee absolute safety or confidentiality to an informant.

604.3.2 JUVENILE INFORMANTS

The use of juvenile informants under the age of 13-years is prohibited.

In all cases, a juvenile 13 years of age or older may only be used as an informant with the written consent of each of the following:

- (a) The juvenile's parents or legal guardians
- (b) The juvenile's attorney, if any
- (c) The court in which the juvenile's case is being handled, if applicable
- (d) The Chief of Police or the authorized designee

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Informants

604.3.3 INFORMANT AGREEMENTS

All informants are required to sign and abide by the provisions of the designated department informant agreement. The officer using the informant shall discuss each of the provisions of the agreement with the informant.

Details of the agreement are to be approved in writing by a supervisor before being finalized with the informant.

604.4 INFORMANT INTEGRITY

To maintain the integrity of the informant process, the following must be adhered to:

- (a) The identity of an informant acting in a confidential capacity shall not be withheld from the Chief of Police, Division Commander, Street Crimes Unit supervisor or their authorized designees.
 - 1. Identities of informants acting in a confidential capacity shall otherwise be kept confidential.
- (b) Criminal activity by informants shall not be condoned.
- (c) Informants shall be told they are not acting as police officers, employees or agents of the South Salt Lake Police Department, and that they shall not represent themselves as such.
- (d) The relationship between department members and informants shall always be ethical and professional.
 - 1. Members shall not become intimately involved with an informant.
 - 2. Social contact shall be avoided unless it is necessary to conduct an official investigation, and only with prior approval of the Street Crimes Unit supervisor.
 - 3. Members shall neither solicit nor accept gratuities or engage in any private business transaction with an informant.
- (e) Officers shall not meet with informants in a private place unless accompanied by at least one additional officer or with prior approval of the Street Crimes Unit supervisor.
 - 1. Officers may meet informants alone in an occupied public place, such as a restaurant.
- (f) When contacting informants for the purpose of making payments, officers shall arrange for the presence of another officer.
- (g) In all instances when department funds are paid to informants, a voucher shall be completed in advance, itemizing the expenses.
- (h) Since the decision rests with the appropriate prosecutor, officers shall not promise that the informant will receive any form of leniency or immunity from criminal prosecution.

604.4.1 UNSUITABLE INFORMANTS

The suitability of any informant should be considered before engaging him/her in any way in a covert or other investigative process. Members who become aware that an informant may be unsuitable will notify the supervisor, who will initiate a review to determine suitability. Until a

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Informants

determination has been made by a supervisor, the informant should not be used by any member. The supervisor shall determine whether the informant should be used by the Department and, if so, what conditions will be placed on his/her participation or any information the informant provides. The supervisor shall document the decision and conditions in file notes and mark the file "unsuitable" when appropriate.

Considerations for determining whether an informant is unsuitable include, but are not limited to, the following:

- (a) The informant has provided untruthful or unreliable information in the past.
- (b) The informant behaves in a way that may endanger the safety of an officer.
- (c) The informant reveals to suspects the identity of an officer or the existence of an investigation.
- (d) The informant appears to be using his/her affiliation with this department to further criminal objectives.
- (e) The informant creates officer-safety issues by providing information to multiple law enforcement agencies simultaneously, without prior notification and approval of each agency.
- (f) The informant engages in any other behavior that could jeopardize the safety of officers or the integrity of a criminal investigation.
- (g) The informant commits criminal acts subsequent to entering into an informant agreement.

604.5 INFORMANT FILES

Informant files shall be utilized as a source of background information about the informant, to enable review and evaluation of information provided by the informant, and to minimize incidents that could be used to question the integrity of department members or the reliability of the informant.

Informant files shall be maintained in a secure area within the Street Crimes Unit. The Street Crimes Unit supervisor or the authorized designee shall be responsible for maintaining informant files. Access to the informant files shall be restricted to the Chief of Police, Division Commander, Street Crimes Unit supervisor or their authorized designees.

The Investigation Division Commander should arrange for an audit using a representative sample of randomly selected informant files on a periodic basis, but no less than one time per year. If the Street Crimes Unit supervisor is replaced, the files will be audited before the new supervisor takes over management of the files. The purpose of the audit is to ensure compliance with file content and updating provisions of this policy. The audit should be conducted by a supervisor who does not have normal access to the informant files.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Informants

604.5.1 FILE SYSTEM PROCEDURE

A separate file shall be maintained on each informant and shall be coded with an assigned informant control number. An informant history shall be prepared to correspond to each informant file and include the following information:

- (a) Name and aliases
- (b) Date of birth
- (c) Physical description: sex, race, height, weight, hair color, eye color, scars, tattoos or other distinguishing features
- (d) Photograph
- (e) Current home address and telephone numbers
- (f) Current employers, positions, addresses and telephone numbers
- (g) Vehicles owned and registration information
- (h) Places frequented
- (i) Briefs of information provided by the informant and his/her subsequent reliability
 1. If an informant is determined to be unsuitable, the informant's file is to be marked "unsuitable" and notations included detailing the issues that caused this classification
- (j) Name of officer initiating use of the informant
- (k) Signed informant agreement
- (l) Update on active or inactive status of informant

604.6 INFORMANT PAYMENTS

No informant will be told in advance or given an exact amount or percentage for his/her service. The amount of funds to be paid to any informant will be evaluated against the following criteria:

- The extent of the informant's personal involvement in the case
- The significance, value or effect on crime
- The value of assets seized
- The quantity of the drugs or other contraband seized
- The informant's previous criminal activity
- The level of risk taken by the informant

The Street Crimes Unit supervisor will discuss the above factors with the Patrol Division Commander and recommend the type and level of payment subject to approval by the Chief of Police.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Informants

604.6.1 PAYMENT PROCESS

Approved payments to an informant should be in cash using the following process:

- (a) Payments of \$500 and under may be paid in cash from a Street Crimes Unit buy/expense fund.
 - 1. The Street Crimes Unit supervisor shall sign the voucher for cash payouts from the buy/expense fund.
- (b) Payments exceeding \$500 shall be made by issuance of a check, payable to the officer who will be delivering the payment.
 - 1. The check shall list the case numbers related to and supporting the payment.
 - 2. A written statement of the informant's involvement in the case shall be placed in the informant's file.
 - 3. The statement shall be signed by the informant verifying the statement as a true summary of his/her actions in the case.
 - 4. Authorization signatures from the Chief of Police and the Mayor are required for disbursement of the funds.
- (c) To complete the payment process for any amount, the officer delivering the payment shall complete a cash transfer form.
 - 1. The cash transfer form shall include the following:
 - (a) Date
 - (b) Payment amount
 - (c) South Salt Lake Police Department case number
 - (d) A statement that the informant is receiving funds in payment for information voluntarily rendered.
 - 2. The cash transfer form shall be signed by the informant.
 - 3. The cash transfer form will be kept in the informant's file.

604.6.2 REPORTING OF PAYMENTS

Each informant receiving a cash payment shall be advised of his/her responsibility to report the cash to the Internal Revenue Service (IRS) as income. If funds distributed exceed \$600 in any reporting year, the informant should be provided IRS Form 1099 (26 CFR 1.6041-1). If such documentation or reporting may reveal the identity of the informant and by doing so jeopardize any investigation, the safety of officers or the safety of the informant (26 CFR 1.6041-3), then IRS Form 1099 should not be issued.

In such cases, the informant shall be provided a letter identifying the amount he/she must report on a tax return as "other income" and shall be required to provide a signed acknowledgement of receipt of the letter. The completed acknowledgement form and a copy of the letter shall be retained in the informant's file.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Informants

604.6.3 AUDIT OF PAYMENTS

The Street Crimes Unit supervisor or the authorized designee shall be responsible for compliance with any audit requirements associated with grant provisions and applicable state and federal law.

At least once every six months, the Chief of Police or the authorized designee should conduct an audit of all informant funds for the purpose of accountability and security of the funds. The funds and related documents (e.g., buy/expense fund records, cash transfer forms, invoices, receipts and logs) will assist with the audit process.

Accountability and Case Management

605.1 ACCOUNTABILITY FOR INVESTIGATIONS

In most cases, the patrol section personnel will conduct preliminary investigations on matters reported to the police department.

- (a) Upon completion of preliminary investigation and report, the shift supervisor will make a determination concerning the follow-up disposition of the case.
 - 1. Investigations that cannot be conducted by officers of the patrol section due to time, lack of resources, and/or expertise, will be referred to the detective section for further follow-up.
- (b) The detective section may initiate preliminary investigations of a uniquely administrative or sensitive nature that do not require an immediate response.
 - 1. Such investigations include, but are not limited to, vice, white-collar crimes, and/or special/covert operations.
- (c) It will be the responsibility of the detective assigned to complete the follow-up investigation to maintain an accurate record of the follow-up investigation.
 - 1. Such records serve to establish investigative continuity.

605.1.1 CASE FILE MANAGEMENT

- (a) All cases forwarded to the detective section will initially be assigned and then designated after review by the Investigation Section Sergeant.
 - 1. In order to facilitate case management and control, where practical, case assignments should be made based on expertise of the detective.
 - 2. Assigned cases will be designated:
 - (a) Active - The case has been assigned and investigative efforts are ongoing, with at least one active lead
 - (b) Inactive - The case has not been brought to a satisfactory conclusion and all case leads have been exhausted.
 - (c) Closed- The case investigation has concluded satisfactorily.
 - (d) Cleared - The case investigation has been completed, identified suspect(s) have been charged, and judicial proceedings are or will be taking place.
 - 3. All cases assigned to a detective will be thoroughly reviewed and the victim and witnesses contacted. prior to any designation being assigned.
 - (a) This shall be done in an attempt to determine if there is any additional information available that was not known or provided at the time of the initial report.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Accountability and Case Management

- (b) All information concerning contacts with the victim and witnesses will be documented by means of supplemental reports.
- (b) The Investigations section Sergeant will maintain a record of all cases assigned for investigation. Such records will at a minimum document the following:
 - (a) Name of the case manger.
 - (b) Date assigned.
 - (c) Case number.
 - (d) Case review date.
- (c) At least monthly, the Investigation Section Sergeant will report to the Division Commander on:
 - (a) The number of cases assigned to the section.
 - (b) The number of cases closed.
 - (c) The number of cases cleared (arrest, warrant etc.)
 - (d) The number of cases inactivated.
 - (e) Any updated information relative to any on-going "major cases".

Eyewitness Identification

606.1 PURPOSE AND SCOPE

This policy sets forth guidelines to be used when members of this department employ eyewitness identification techniques.

606.1.1 DEFINITIONS

Definitions related to the policy include:

Eyewitness identification process- Any field identification, live lineup or photographic identification.

Field identification - A live presentation of a single individual to a witness following the commission of a criminal offense for the purpose of identifying or eliminating the person as the suspect.

Live lineup -A live presentation of individuals to a witness for the purpose of identifying or eliminating an individual as the suspect.

Photographic lineup - Presentation of photographs to a witness for the purpose of identifying or eliminating an individual as the suspect.

606.2 POLICY

This department will strive to use eyewitness identification techniques, when appropriate, to enhance the investigative process and will emphasize identifying persons responsible for crime and exonerating the innocent.

606.3 INTERPRETIVE SERVICES

Officers should make a reasonable effort to arrange for an interpreter before proceeding with eyewitness identification if communication with a witness is impeded due to language or hearing barriers.

Before the interpreter is permitted to discuss any matter with the witness, the investigating officer should explain the identification process to the interpreter. Once it is determined that the interpreter comprehends the process and can explain it to the witness, the eyewitness identification may proceed as provided for within this policy.

606.4 EYEWITNESS IDENTIFICATION FORM

The Investigation supervisor shall be responsible for the development and maintenance of an eyewitness identification process for use by members when they are conducting eyewitness identifications.

The process and any related forms or reports should provide:

- (a) The date, time and location of the eyewitness identification procedure.
- (b) The name and identifying information of the witness.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Eyewitness Identification

- (c) The name of the person administering the identification procedure.
- (d) If applicable, the names of all of the individuals present during the identification procedure.
- (e) An admonishment that the suspect may or may not be among those presented and that the witness is not obligated to make an identification.
- (f) An admonishment to the witness that the investigation will continue regardless of whether identification is made by the witness.

The process and related forms should be reviewed at least annually and modified when necessary.

606.5 EYEWITNESS IDENTIFICATION

Officers are cautioned not to, in any way, influence a witness as to whether any subject or photo presented in a lineup is in any way connected to the case. Officers should avoid mentioning that:

- The individual was apprehended near the crime scene.
- The evidence points to the individual as the suspect.
- Other witnesses have identified, or failed to identify, the individual as the suspect.

In order to avoid undue influence, witnesses should view suspects or a lineup individually and outside the presence of other witnesses. Witnesses should be instructed to avoid discussing details of the incident or of the identification process with other witnesses.

Whenever feasible, the eyewitness identification procedure should be audio and/or video recorded and the recording should be retained according to current evidence procedures.

606.5.1 PHOTOGRAPHIC LINEUP AND LIVE LINEUP CONSIDERATIONS

When practicable, the person composing the lineup and the person presenting the lineup should not be directly involved in the investigation of the case. When this is not possible, the member presenting the lineup must take the utmost care not to communicate the identity of the suspect in any way.

When practicable, the employee presenting a lineup to a witness should not know which photograph or person is the suspect.

Other persons or photos used in any lineup should bear similar characteristics to the suspect to avoid causing him/her to unreasonably stand out. In cases involving multiple suspects, a separate lineup should be conducted for each suspect. The suspects should be placed in a different order within each lineup.

The employee presenting the lineup to a witness should do so sequentially and not simultaneously (i.e., show the witness one person at a time). The witness should view all persons in the lineup.

The order of the suspect or the photos and the fillers should be randomized before being presented to each witness.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Eyewitness Identification

A live lineup should only be used before criminal proceedings have been initiated against the suspect. If there is any question as to whether any criminal proceedings have begun, the investigating officer should contact the appropriate prosecuting attorney before proceeding.

606.5.2 FIELD IDENTIFICATION CONSIDERATIONS

Field identifications, also known as field elimination show-ups or one-on-one identifications, may be helpful in certain cases. A field elimination or show-up identification should not be used when independent probable cause exists to arrest a suspect. In such cases a live or photo lineup is the preferred course of action if eyewitness identification is contemplated.

When initiating a field identification, the officer should observe the following guidelines:

- (a) Obtain a complete description of the suspect from the witness.
- (b) Assess whether a witness should be included in a field identification process by considering:
 - 1. The length of time the witness observed the suspect.
 - 2. The distance between the witness and the suspect.
 - 3. Whether the witness could view the suspect's face.
 - 4. The quality of the lighting when the suspect was observed by the witness.
 - 5. Whether there were distracting noises or activity during the observation.
 - 6. Any other circumstances affecting the witness's opportunity to observe the suspect.
 - 7. The length of time that has elapsed since the witness observed the suspect.
- (c) If safe and practicable, the person who is the subject of the show-up should not be handcuffed or in a patrol vehicle.
- (d) When feasible, officers should bring the witness to the location of the suspect, rather than bring the suspect to the witness.
- (e) A person should not be shown to the same witness more than once.
- (f) In cases involving multiple suspects, witnesses should only be permitted to view the suspects one at a time.
- (g) A person in a field identification should not be required to put on clothing worn by the suspect, to speak words uttered by the suspect or to perform other actions mimicking those of the suspect.
- (h) If a witness positively identifies an individual as the perpetrator, officers should not conduct any further field identifications with other witnesses for that suspect. In such instances officers should document the contact information for any additional witnesses for follow up, if necessary.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Eyewitness Identification

606.6 DOCUMENTATION

A thorough description of the eyewitness process and the results of any eyewitness identification should be documented in the case report. Witness comments of how certain he/she is of the identification or non-identification should be quoted in the report.

If a photographic lineup is utilized, a copy of the photographic lineup presented to the witness should be included in the case report. In addition, the order in which the photographs were presented to the witness should be documented in the case report.

Investigative Task Forces

607.1 PURPOSE AND SCOPE

- (a) Realizing that some criminal activity may require major investigative efforts or may involve multiple jurisdictions, the South Salt Lake City Police Department willingly participates in task forcing its available resources with other agencies in order to combat crime that affects the safety and well being of the community.
- (b) The investigative task force may consist of personnel from the various organizational components of the South Salt Lake City Police Department, or it may involve personnel from various local, state, and federal law enforcement agencies.
- (c) If a multi-agency task force is formed, the directors of the agencies involved shall sign a written agreement. In most cases this agreement will consist of a "Resolution" prepared by the City Attorney, approved by the South Salt Lake City Council, signed by the Council Chair and the Mayor.

Brady Material Disclosure

608.1 PURPOSE AND SCOPE

This policy establishes guidelines for identifying and releasing potentially exculpatory or impeachment information (so-called “*Brady* information”) to a prosecuting attorney.

608.1.1 DEFINITIONS

Definitions related to this policy include:

Brady information - Information known or possessed by the South Salt Lake Police Department that is both favorable and material to the current prosecution or defense of a criminal defendant, including potential impeachment information relating to the conduct of an officer who was involved in the arrest or investigation of the defendant (Utah Code 53-25-1001).

608.2 POLICY

The South Salt Lake Police Department will conduct fair and impartial criminal investigations and will provide the prosecution with both incriminating and exculpatory evidence, as well as information that may adversely affect the credibility of a witness. In addition to reporting all evidence of guilt, the South Salt Lake Police Department will assist the prosecution by complying with its obligation to disclose information that is both favorable and material to the defense. The [Department/Office] will identify and disclose to the prosecution potentially exculpatory information, as provided in this policy.

608.3 DISCLOSURE OF INVESTIGATIVE INFORMATION

Officers must include in their investigative reports adequate investigative information and reference to all material evidence and facts that are reasonably believed to be either incriminating or exculpatory to any individual in the case. If an officer learns of potentially incriminating or exculpatory information any time after submission of a case, the officer or the handling investigator must prepare and submit a supplemental report documenting such information as soon as practicable. Supplemental reports shall be promptly processed and transmitted to the prosecutor's office.

If information is believed to be privileged or confidential (e.g., confidential informant or attorney-client information, attorney work product), the officer should discuss the matter with a supervisor and/or prosecutor to determine the appropriate manner in which to proceed.

Evidence or facts are considered material if there is a reasonable probability that they would affect the outcome of a criminal proceeding or trial. Determining whether evidence or facts are material often requires legal or even judicial review. If an officer is unsure whether evidence or facts are material, the officer should address the issue with a supervisor.

Supervisors who are uncertain about whether evidence or facts are material should address the issue in a written memo to an appropriate prosecutor. A copy of the memo should be retained in the [Department/Office] case file.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Brady Material Disclosure

608.4 DISCLOSURE OF PERSONNEL INFORMATION

If a member of this [department/office] is a material witness in a criminal case, a person or persons designated by the Chief of Police shall examine the personnel file and/or internal affairs file of the officer to determine whether they contain *Brady* information. If *Brady* information is located, the following procedure shall apply:

- (a) In the event that a motion has not already been filed by the criminal defendant or other party, the prosecuting attorney and [department/office] member shall be notified of the potential presence of *Brady* material in the member's personnel file.
- (b) The prosecuting attorney or [department/office] counsel should be requested to file a motion in order to initiate an in-camera review by the court (Utah Code 63G-2-202(7)).
 - 1. If no motion is filed, the supervisor should work with counsel to determine whether the records should be disclosed to the prosecutor.
- (c) The Custodian of Records shall accompany all relevant personnel files during any in-camera inspection to address any issues or questions raised by the court.
- (d) If the court determines that there is relevant *Brady* material contained in the files, only that material ordered released will be copied and released to the parties filing the motion.
 - 1. Prior to the release of any materials pursuant to this process, the Custodian of Records should request a protective order from the court limiting the use of such materials to the involved case and requiring the return of all copies upon completion of the case.
- (e) If a court has determined that relevant *Brady* information is contained in the member's file in any case, the prosecutor should be notified of that fact in all future cases involving that member.

The person or persons designated by the Chief of Police should periodically examine the personnel files and/or internal affairs files of all officers who may be material witnesses in criminal cases to determine whether they contain *Brady* information. The obligation to provide *Brady* information is ongoing. If any new *Brady* information is identified, the prosecuting attorney should be notified.

608.5 INVESTIGATING BRADY ISSUES

If the [Department/Office] receives information from any source that a member may have issues of credibility or dishonesty or has been engaged in an act of moral turpitude or criminal conduct, the information shall be investigated and processed in accordance with the Personnel Complaints Policy (Utah Code 53-25-1003).

608.5.1 GROUNDS FOR DISCIPLINARY ACTION

Placement on a prosecuting agency's *Brady* identification system shall not be the sole reason for disciplinary action to be taken against an officer. However, the underlying facts that were the basis for placement, or the failure to disclose such placement to another prosecuting agency

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Brady Material Disclosure

when required by law, may lead to disciplinary action against the officer in accordance with the Personnel Complaints Policy (Utah Code 53-25-1003).

608.6 SUBPOENA PROCESSING

The individual processing subpoenas (or the supervisor of the subpoenaed member) shall check the subpoenaed member's name against the current list of those who are known to have *Brady* information in their files or background, and shall alert the coordinator if a person on the list is subpoenaed.

608.6.1 DISCLOSURE TO PROSECUTING AGENCY

As soon as practicable after receiving a subpoena to testify in court by a prosecuting agency, an officer who has been placed onto a *Brady* identification system of a different prosecuting agency shall disclose that placement to the prosecuting agency that issued the subpoena (Utah Code 53-25-1003).

608.7 TRAINING

[Department/Office] personnel should receive periodic training on the requirements of this policy.

Investigative Polygraphs

609.1 PURPOSE AND SCOPE

- (a) Since the use of the polygraph may be generally perceived by the public as an indication of guilt, it is the policy of the South Salt Lake City Police Department not to release any information regarding the use of or results from a polygraph examination during an investigation.
 - 1. The decision to employ polygraph examinations during the course of a criminal investigation resides with the Chief of Police or designee.
 - 2. The decision whether or not to use polygraph examinations for pre-employment, internal investigation, assisting outside agencies, or other non-criminal matters resides with the Chief of Police or designee.
- (b) When authorizing an polygraph examination, the approving authority should determine that an investigation by other means has been as thorough as circumstances reasonably permit.
 - 1. It should be recognized that the effectiveness and accuracy of a polygraph examination are greatest when the examiner's knowledge relevant points of the matter under investigation have been narrowed and well defined.
- (c) Investigative polygraphs will only be administered by examiners who have satisfactorily completed training from and are certified by a polygraph school accredited by the American Polygraph Association.

Pawn Shop Holds

610.1 PURPOSE AND SCOPE

Property with evidentiary value is often found at pawn shops and secondhand businesses. Utah law allows the South Salt Lake Police Department to seize or place a hold on such property. This policy provides guidance on placing such holds.

610.2 POLICY

The South Salt Lake Police Department will place a hold on an item that has evidentiary value and is in the possession of a pawn or secondhand business only as allowed by Utah law and when the item is necessary to an open investigation.

610.3 PROCEDURE

A member of the Department may require a pawnbroker or secondhand business to place a 90-day hold on an item in the possession of the pawnbroker or secondhand business if the item is necessary to an open investigation. The hold may be extended for an additional 90 days if warranted. Subsequent extensions must be approved by a court order (Utah Code 13-32a-109).

An officer may seize the held item when exigent circumstances exist or when necessary during the course of a criminal investigation. Items may also be seized (Utah Code 13-32a-109.5; Utah Code 13-32a-115(2)):

- (a) When seizure is necessary to permit the fingerprinting or chemical testing of the item.
- (b) If the item contains unique or sensitive personal identifying information.

A written hold or seizure notice shall be provided and shall include (Utah Code 13-32a-109.5):

- An active case number.
- The date of the hold or seizure request and the property to be held or seized.
- Notice to the pawnbroker or secondhand business of contact information to allow tracking of the property when the prosecuting agency takes over the case.
- If the property is seized, the reason the property is necessary during the course of a criminal investigation.

If the pawnbroker or secondhand business is located outside of the jurisdiction of this department, a copy of the hold notice shall be sent to the local law enforcement agency having jurisdiction (Utah Code 13-32a-109). An extension of the hold must be communicated in writing to the pawnbroker or secondhand business prior to the expiration of the initial 90-day hold (Utah Code 13-32a-109).

Whenever the officer has reason to believe that property subject to a hold is in the possession of a pawnbroker or secondhand business, the officer should notify the person who reported the property as lost or stolen, as well as any agency taking a report, of all of the following:

- The name, address, and telephone number of the pawnbroker or secondhand business that reported the acquisition of the property or where the property is located.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Pawn Shop Holds

- The length of any holding period.

610.4 TERMINATION OF HOLD

The evidence supervisor should maintain a file copy of all hold notices and should review the file at least every 30 days for pending expirations. When the need for the hold or seizure of an item is terminated and no original victim was located, the Department shall, within 15 business days after the termination (Utah Code 13-32a-109(7)):

- (a) Notify the pawnbroker or secondhand business in writing that the hold or seizure has been terminated.
- (b) Return the item to the pawnbroker or secondhand business, or advise the pawnbroker or secondhand business, either in writing or electronically, of the specific alternative disposition of the item.

If an original victim was located, the release of the property shall only be made with the consent of the appropriate prosecutor and with notices made according to Utah Code 13-32a-109(8).

If this Department receives a registered or certified letter from the pawnbroker or secondhand business informing the Department that the holding period has expired, the Department shall respond within 30 days in the manner prescribed by law (Utah Code 13-32a-109(9)).

610.5 TRAINING

The Training Coordinator should ensure that members with access to the Utah Division of Consumer Protection's central database for pawnbrokers and secondhand business (Utah Code 13-32a-105) receive annual training related to property held by pawn shops and secondhand businesses (Utah Code 13-32a-112.1).

Sensitive Complaint Processing

611.1 PURPOSE AND SCOPE

Complaints alleging vice or organized criminal activity may be received by any employee of this agency and forwarded to the detective section using the department case report form. If the original complaint was received from an informant, the information will be forwarded to the Detective Sergeant for an evaluation of the submitted information as directed by Policy.

611.1.1 PROCEDURE

- (a) Whenever possible, the detective section will be responsible for conducting both the preliminary and follow-up investigation of any reported organized crime and vice activity. The Investigation Section Sergeant will assign the case to a detective with specific investigative skills concerning the crime.
- (b) A Division Commander will be notified under circumstances in which the patrol division has initiated organized crime and/or vice investigation.
- (c) As determined by the Investigations Division Commander, reports of a very sensitive nature will not be forwarded to the records section until the case is completed.
 - 1. Cases of sensitive nature may be assigned a case number through VECC.
 - 2. The report will be secured by the detective in a locked filing cabinet until completion until the completion of the case, at which time it will be forwarded to the records section.
 - 3. The Investigation Section Commander or Sergeant will make notification to the police M.I.S. Sergeant and request the case be "partitioned" in the Records Management System.
 - 4. Only the detective and supervisory chain of command shall have access to the file.
- (d) Investigative methods employed in the course of vice and organized crime investigations may include:
 - 1. Surveillance and/or stakeout.
 - 2. Undercover operatives.
 - 3. Electronic surveillance (pursuant to court order).
 - 4. Informants.
 - 5. Communication with other local, state, and/or federal enforcement agencies.
- (e) All methods employed shall be recorded and maintained in the investigative file.
- (f) Notifications:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Sensitive Complaint Processing

1. Victims associated with vice and organized criminal activities will be notified of the status of their case as it pertains to the arrest of suspects, suspension or closing of an investigation.
2. Complainants/witnesses involved in vice and organized crime cases may be notified of developments in the investigative process on a "need to know" basis. Final determination concerning the release of information to such persons will be made by the investigations section supervisor.
3. Any employee of the South Salt Lake City Police Department, who acquires knowledge/information concerning vice/organized crime activity, shall notify his/her supervisor immediately.
 - (a) Reports of such activity will be directed through the employee's immediate supervisor to the Chief of Police or designee.

611.1.2 SENSITIVE INVESTIGATION RECORD HANDLING

- (a) The South Salt Lake Police Department shall take measures to ensure security of records found to be sensitive. The determination as to whether a record should be considered sensitive shall be the responsibility of the Chief of Police or designee. Types of cases which should be considered for handling as a sensitive investigation include, but are not limited to:
 1. Vice.
 2. Narcotics.
 3. Organized Crime.
 4. Internal Affairs.
 5. Others as determined by the Chief of Police or designee.
- (b) The nature of these types of crimes, and the considerable amount of undercover work involved in controlling these offenses, contribute to the sensitivity of related records.
- (c) Records which are determined to be sensitive, shall be kept secure, should be maintained separately or "partitioned" from the central Records Management System, and may only be accessed by authorized personnel.

611.1.3 INVESTIGATIVE FUNDS

- (a) An investigative fund will be established for the purpose of supporting investigations related to vice, organized crime control operations, narcotics investigations and any other criminal investigations deemed appropriate by the Office of the Chief of Police.
 1. Monies drawn from this fund may be used for activities such as payment of informants, purchasing contraband as evidence, surveillance activities and

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Sensitive Complaint Processing

equipment. The control of operation of this fund will be the responsibility of the Deputy Chief of Police.

2. Refer to South Salt Lake City Police Department Policy and Procedures, Chapter 8, 821 and Chapter 6, 608 concerning specific policies governing the use of and accounting for investigative funds.
3. The Deputy Chief of Police is responsible for the issuance of investigative funds.

Special Operations Procedures

612.1 PURPOSE AND SCOPE

- (a) The following provisions may apply when conducting vice, drug, crime surveillance, undercover, decoy, and raid operations:
 - 1. Analysis of crimes, victims, and suspects.
 - 2. Determination of legal ramifications.
 - 3. Familiarization of officers with the objectives and details of the operation, the neighborhood, or target area.
 - 4. Determination of operational procedures for observation, arrests, surveillance, and high-risk entries
 - 5. Supplying of officers with expense funds.
 - 6. Establishment of means of routine and emergency communications.
 - 7. Selection of equipment or vehicles.
 - 8. Provision of relief, backup security, and perimeter protection for officers.
 - 9. Supplying of officers with false identity, disguises, and necessary credentials.
 - 10. Maintenance of overall confidentiality and cover.
 - 11. Obtaining of authorization for the raid and use of force.
 - 12. Designation of a single person as supervisor and coordinator.
 - 13. Provision of close supervision.
 - 14. Making contacts with suspects.
 - 15. Searching for and seizure of evidence and/or contraband.
 - 16. Requesting for medical assistance, if needed.
 - 17. Obtaining coordination and assistance from others both inside and outside of the agency.

612.1.1 SURVEILLANCE OPERATIONS

- (a) Surveillance operations will be preceded by a thorough analysis of the alleged crimes and victims involved. Such an analysis may yield information necessary to conduct a safe and effective surveillance operation.
 - 1. Surveillance operations will be preceded by an analysis of the probable offenders, to include, but not limited to:
 - (a) Habits.
 - (b) Associates.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Special Operations Procedures

- (c) Vehicles.
 - (d) Methods of operation
 - (e) Address.
 - (f) Employment.
 - (g) And hazard factor(s).
- (b) Prior to conducting surveillance operations, operatives will be familiarized with the target area(s).
- (c) Surveillance operations should be conducted in such a manner that the observation and/or "tailing" of a suspect is accomplished while presenting as little, if any, intrusion to people and surroundings nearby. As circumstances dictate, arrests will be made with as limited exposure of police presence as possible.
- (d) Funds necessary to support the activities of operatives engaged in surveillance operations will be allocated in accordance with the provisions outlined in South Salt Lake Police Department Policy and Procedure, Chapter 8 821 & Chapter 6, 608.
- (e) Surveillance operations planning will include provisions for communications among operatives. Such provisions may include radio transceivers, pagers, telephones, hand signals, and other means necessary, as circumstances require.
- (f) Vehicles used during surveillance operations should be of a make and model that will not present the image of police agency, e.g. "fleet purchase" type vehicles.
 - (a) Vehicles should be interchanged between operative in order that surveillance "patterns" are not established, and become evident to the objects of the surveillance.
 - (b) Vehicles and equipment should be used in such a manner that counter-surveillance measures by suspects are negated.
- (g) Supervisor's who are responsible for coordinating surveillance operations will consider those factors necessary to provide food and rest for operatives during the operation.
- (h) Supervisors responsible for the planning of surveillance operations will evaluate all pertinent legal issues as they apply to the operational plan of action. If legal concerns arise, the supervisor can consult with The District Attorney's Office and/or the City Attorney's Office.
- (i) Undercover operations are an acceptable alternative means used during investigations of vice and organized crime.
 - (a) The decision to use undercover operations, as for any other method, is to be based on the factors and circumstances relating to a particular investigation.
 - (b) The safety of those involved will be a specific and constant factor for consideration in any undercover operation.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Special Operations Procedures

612.1.2 UNDERCOVER OPERATIONS

- (a) Undercover operations require approval of the Chief of Police or designee. The supervisor of the unit proposing undercover operations must be able to demonstrate that planning has been conducted that addresses:
 - 1. Identification and examination of the activities of known or possible suspects.
 - 2. Method to be used in contacting suspects.
 - 3. Analysis of target area where operations will be conducted.
 - 4. The requirement for undercover operations in conducting the investigation.
 - 5. Method to be used in maintaining confidentiality of undercover officer's false identity.
- (b) After an undercover operation is approved, the supervisor of the unit conducting the operation will be responsible for arranging the undercover officers:
 - 1. Credentials and false identities.
 - 2. Expense funds.
 - 3. Equipment.
- (c) The supervisor of the unit conducting the operation will be responsible for coordinating with the Investigation Section Sergeant to determine the legal and operational use, maintenance and return of the equipment.
 - 1. This will ensure a central point for coordination of the use of the equipment so that it can be made available during the planning stages of the operation and not conflict with other operations where the equipment is required.
- (d) Special attention will be given to ensuring that all officers involved are thoroughly briefed on:
 - 1. The means established for routine and emergency communications (including duress signals).
 - 2. Procedures for security of the undercover officers.
 - 3. When and how any arrests will be affected.
- (e) Considering the technicalities and complexities of law enforcement undercover operations, legal assistance and advice from the office of the District Attorney or City Attorney's Office should be an integral part of any operation where unusual circumstances are encountered.
- (f) Supervisors are charged with maintaining close supervision of undercover operations.

612.1.3 DECOY OPERATIONS

- (a) The decision to initiate a decoy operation will be based on an analysis of crimes, victims, locations, frequency of activity, probable offenders, methods of operation, and any other pertinent information.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Special Operations Procedures

- (b) All decoy operations will be directed and closely monitored by a supervisor. It shall be that supervisor's responsibility to ensure that:
 - 1. Decoy officers are selected and equipped with the intent that they resemble the victims as much as possible.
 - 2. No decoy officer shall be placed without an adequate number of backup officers nearby in visual and/or verbal contact.
 - 3. Action or "bust" signals and emergency signals will be made known to, and acknowledged by, all personnel prior to the beginning of the operation.
 - 4. All decoy operation plans are reviewed with City Attorney's or District Attorney's office, prior to beginning operation.
 - 5. All personnel involved in the operation are thoroughly briefed and are aware of their assigned specific duties and responsibilities.
 - 6. Any special equipment needed is available and in good working order and is operated by qualified personnel.
 - 7. The supervisor in charge of the on-duty patrol shift and the dispatcher on duty are notified in advance of the start of any decoy operation and consulted regarding any participation required from their personnel.

612.1.4 VICE AND ORGANIZED CRIME INVESTIGATION

- (a) Vice and organized crime raids by the detective section will not be conducted without:
 - 1. The authorization of the Chief of Police or designee.
 - 2. The direction of a Division Commander or designee.
 - 3. The respective Division Commander will notify the on-duty patrol (and any other affected) supervisor as well in the event a operation is planned or initiated.
 - 4. The Chief of Police, or designee, will be notified for approval in the event that special response is required in support of vice and organized crime operations.
- (b) Prior to approaching or entering a targeted area where a vice or organized crime search is to occur, measures should be taken to insert an undercover operative into the area for the purposes of surveillance and reporting the activities of suspects or other hostile elements.
- (c) Unless circumstances suggest that officer safety would be jeopardized, the announcement of police presence in a targeted area will be made at the time of a operation.
- (d) Conducting unannounced ("no knock") entry should be done only when necessary to preserve evidence, or reduce the threat in apprehending clearly dangerous persons. Authorization for unannounced ("no knock") entry:
 - 1. Make such entries in the safest manner possible.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Special Operations Procedures

2. Authorization will almost always be achieved by obtaining a search warrant that includes provisions for such entry.
 3. Exigent circumstances may preclude obtaining the warrant in a timely manner. In these cases entry is made only to secure the area to preserve evidence until a warrant is obtained.
 4. These same exigent circumstances may interfere with the normal planning process covered in this operating procedure. However, even in exigent circumstances, provisions of this operating procedure shall be followed to the extent practical.
 5. Some public buildings or public areas in private structures may not require search warrants. Authorization from a police supervisor is required to conduct a search in a place where a warrant is not required.
 6. With the exception of undercover operatives, officers engaged in search operations will be uniformed or in some other obvious manner identified as police.
- (e) Upon completion of a search, steps should be taken to secure buildings, vehicles, and structures which may have become unsecured during the search.
- (f) The selection of special units needed to support organized crime and/or vice raid operations will be the responsibility of a division commander or their designee, and will require a plan of action outlining provisions for communications during all operations.
- (g) Vice and organized crime search planning will include provision for the arrest and processing of suspects.
1. The transportation, processing, and care of arrested persons will be conducted in as safe and efficient manner as possible.
 2. In order to ensure an efficient and organized booking process, one officer/detective will be designated as the primary booking official.
- (h) The use of force during vice and/or organized crime search will be in accordance with UCA, 76-2-404.
- (i) Pre-established fire response conditions will be authorized by the supervisor/commander only.
1. Fire and aid units should be put on standby status.
 2. These units may be summoned to a staging area or other safe area at the discretion of the incident commander.
- (j) All personnel involved will complete necessary reports concerning their activities and assignments during the search. These reports will then be filed under the master case report number assigned to the search.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Special Operations Procedures

612.1.5 AGENCY COOPERATION

- (a) Communication, coordination and cooperation among all other departmental units and outside agencies is essential to the efficiency and effectiveness of the South Salt Lake City Police Department.
 - 1. Personal interaction between detectives and patrol officers is encouraged in order to enhance relationships between the sections and to facilitate the exchange of information.
 - 2. The detective section sergeant will contact the on-duty patrol shift supervisors to maintain a positive rapport and to review cases and information of mutual concern.
 - 3. Detectives will routinely attend a patrol shift roll call for the exchange of information on cases and items of mutual interest and to request assistance as appropriate in the investigation of assigned cases.
 - 4. The "Inter-Departmental Memo" or Electronic Mail form will be utilized by investigators to provide positive feedback to the patrol officers who would otherwise not be advised of the outcome of cases they initiated.
- (b) The department provides various personnel to assist and make contacts within other agencies.
 - 1. These contacts result in a positive relationship with the outside agencies and groups.
 - 2. If the department needs the assistance of an outside agency, the on-call or affected division commander must first be advised and give his/her approval.

612.1.6 CAPACITY FOR CONDUCTING COVERT OPERATIONS

- (a) The South Salt Lake City Police Department may have equipment and trained personnel to conduct covert operations for the control of vice, drug and/or organized crime violations. Such as activity may include, but is not limited to:
 - 1. Infiltration of suspected illegal operations.
 - 2. Decoy operations.
 - 3. Undercover operations.
 - 4. Surveillance operations.
- (b) Covert operations must be reviewed and approved by the Investigations Division Commander before any action is taken.
- (c) All necessary equipment will be obtained according to the previous section.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Special Operations Procedures

- (d) Other agencies within the State of Utah may provide needed equipment and/or personnel, as requested by this agency under the oversight of the Investigations Division Commander or his/her designee.

De-Confliction of Activity or Event

613.1 PURPOSE AND SCOPE

To establish a policy where the South Salt Lake City Police Department will participate in the RISSafe de-confliction system.

613.1.1 POLICY

In an effort to ensure officer safety, as well as to prevent investigative conflicts between different units of the department and other law enforcement agencies, the South Salt Lake City Police Department will enter operational information into the RISSafe program, before any of the following operations are conducted by ANY unit of the Department:

- (a) Undercover buys
- (b) Controlled buys
- (c) Reverse stings
- (d) Search Warrants
- (e) Knock-and-Talks
- (f) Pre-determined stationary surveillance
- (g) Staging locations
- (h) Controlled deliveries
- (i) Non-narcotics undercover activities
- (j) Pre-planned street level narcotics enforcement activities by uniformed officers
- (k) SWAT activities
- (l) or any other law enforcement operation that has potential conflicts with other units of the department or other law enforcement agencies.

613.1.2 NOTIFICATIONS

- (a) Notification of upcoming narcotic, tactical, surveillance or other operation, shall be made through entry into the web based de-confliction software, prior to the event being conducted.
 - 1. The web based system is available 24 hours a day, seven days a week.
 - 2. If notification cannot be made via the web, notification can be made to the Investigative Support Center (ISC), Monday-Friday (Excluding Holidays) between the hours of 0830 and 1700, by calling _____.
 - 3. If the notification cannot be made via the web or to the ISC, notification can be made to (VECC?, UBI?, RECORDS?) by calling: _____.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

De-Confliction of Activity or Event

4. Any changes that occur during the operation, such as times, locations and spin-off operations, will be updated in the system before the changes are enacted.
 5. Once the operation has been entered into the de-confliction system, an EVENT I.D. NUMBER will be issued, by the system, for the operation.
 6. If the operation is conducted outside the jurisdiction of the South Salt Lake City Police Department, notification shall also be made to the law enforcement agency with jurisdiction over the location of the operation.
- (b) INFORMATION REQUIRED FOR NOTIFICATION "" Includes the following:
1. Date(s).
 2. Time frame.
 3. Address of the operation or nearby intersection.
 4. Type of operation.
 5. Primary agency conducting the operation.
 6. Any other agency participating in the operation.
 7. Primary Officer/Detective name and phone numbers, to include office, cell and pager numbers.
 8. Alternate point of contact, to include office, cell and pager numbers of the alternate contact.
 9. Radius of de-confliction.

613.1.3 DOCUMENTATION

Entry into the de-confliction system will be documented by entering the EVENT I.D. NUMBER in one of the following documents:

- (a) Initial or supplemental report.
- (b) Operation Plan form.

613.1.4 ULEIN

Inquiries to ULEIN must be done when enforcement action is intended on any violator, during an investigation where the de-confliction system is used.

- (a) If concurrent information exists, ULEIN guidelines will be followed.

613.1.5 POTENTIAL CONFLICTS

If the de-confliction system provides notification that there may be a potential conflict with any other operation, contact shall be made with the Officer/Agent of the agency with which the conflict exists.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

De-Confliction of Activity or Event

- (a) This contact must be made prior to the South Salt Lake City Police Department operation being conducted.

Operations Planning and Deconfliction

614.1 PURPOSE AND SCOPE

This policy provides guidelines for planning, deconfliction and execution of high-risk operations, such as search warrants, sting operations and arrest warrant service. The policy also covers the risk mitigation process that should be a part of these activities. South Salt Lake City Police Department will participate in the RISSafe de-confliction system.

614.1.1 DEFINITIONS

Definitions related to this policy include:

Deconfliction - A centralized process that allows for the collection of operations and case information and that provides alerts to enhance safety and avoid duplication or confliction of operations.

Reportable incident - When law enforcement officers use forcible entry to serve a search warrant, or when a special unit that is specifically trained and equipped to respond to critical, high-risk situations within either the Department or an assisting department is deployed (Utah Code 77-7-8.5).

614.2 POLICY

It is the policy of the South Salt Lake Police Department to properly plan and execute large scale and high-risk operations. Proper planning and execution enable effective coordination of such operations. The SSLPD will participate in a regional deconfliction system that is designed to enhance the safety of officers and the public, to decrease the risk of compromising investigations and prevent the duplication of efforts.

614.3 OPERATIONS DIRECTOR

The Chief of Police will designate a member of this department to be the operations director. SSLPD operation director will be the Operations Lieutenant or the Investigative Sergeant. The operations director will develop and maintain a risk assessment form for use in assessing, planning and coordinating high-risk operations. The form also should provide a process for supervisors to identify operations that have a lower level of risk. The UPD SWAT Matrix form will be utilized for all SSLPD operations, to determine the risk and liability.

The director will review risk assessment forms with operations supervisors to determine whether a particular incident qualifies as high risk, and will also have the responsibility of directing high-risk operations.

614.4 DECONFLICTION

The officer who is the operation lead shall ensure the investigative target and location have been entered in the regional target deconfliction system to determine if there is conflicting activity by other agencies involving the same individual, group or location. ULEIN entry into the de-

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Operations Planning and Deconfliction

confliction system will be documented by entering the EVENT I.D. NUMBER in one of the following documents:

- a. Initial or supplemental report.
- b. Operation Plan form.

This should occur as early in the process as practical, but no later than two hours prior to the commencement of the operation. The officer should also enter updated information when it is received. If any conflict is discovered, the supervisor will contact the involved jurisdiction and resolve the potential conflict before proceeding with the operation.

614.5 OPERATION PLAN

The operations director or the authorized designee shall supervise operations that are categorized as high-risk. The director should ensure that a written plan is developed. The plan should address such issues as:

- (a) Operation goals, objectives and strategies.
- (b) Information from the risk assessment form, by attaching a completed copy in the operation plan.
 - 1. The volume or complexity of the information may indicate that the plan includes a synopsis of the information contained on the risk assessment form to ensure clarity and highlighting of critical information.
- (c) Participants and their roles:
 - 1. An adequate number of uniformed officers are included in the operation team to ensure the operation is recognized as a legitimate law enforcement operation.
 - 2. How all participants will be identified as law enforcement.
- (d) Whether deconfliction submissions are current and that all target individuals, groups and locations have been deconflicted to the extent reasonably practicable.
- (e) Identification of communications channels and call-signs.
- (f) Use of force issues.
- (g) Contingencies for handling medical emergencies (e.g., services available at the location, closest hospital, closest trauma center).
- (h) Plans for detaining people who are not under arrest.
- (i) Contingencies for handling children, dependent adults, animals and other people who might be at the location. This should be done in accordance with the Child and Dependent Adult Safety and the Animal Control policies.
- (j) Documentation of actions and responsibilities for collection, review and approval of reports.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Operations Planning and Deconfliction

614.5.1 OPERATION PLAN RETENTION

Since the operation plan contains intelligence information and descriptions of police tactics, it shall not be filed with the police report package. It shall be stored separately and retained in accordance with the established records retention schedule.

614.6 OPERATION BRIEFING

A briefing should be held prior to the commencement of the operation to allow all participants to understand the operation, see and identify each other, identify roles and responsibilities, and to ask questions or seek clarification as needed. Anyone who is not present at the briefing should not be present at the location of the operation without specific supervisory approval.

- (a) The briefing should include a verbal review of the plan's elements, using visual aids, to enhance the participants' understanding of the plan.
- (b) All participants should be provided a copy of the plan and search warrant, if applicable. If a search warrant is being served, participating personnel should be directed to read the search warrant and initial a copy that is retained with the operation plan. Any items to be seized should be identified at the briefing.
- (c) The operations director or supervisor at the briefing shall ensure that all participants are visually identifiable as law enforcement officers.
 - 1. Exceptions may be specifically identified because of a specialized function, such as officers who are conducting surveillance or working undercover. However, those members exempted from visual identification should be able to transition to a visible law enforcement indicator at the time of enforcement actions, such as entries or arrests.
- (d) The briefing should include details of the communications plan.
 - 1. It is the responsibility of the operation supervisor to ensure that Dispatch is notified of the time and location of the operation, and to provide a copy of the operation plan prior to officers arriving at the location.
 - 2. If the radio channel needs to be monitored by Dispatch, the dispatcher assigned to monitor the operation should attend the briefing, if practical, but minimally should receive a copy of the operation plan.
 - 3. The briefing should include a communications check to ensure that all participants are able to communicate with the available equipment on the designated radio channel.

614.7 UNIFIED POLICE DEPARTMENT SPECIAL WEAPONS AND TACTICS TEAM (S.W.A.T.)/CRISIS RESPONSE UNIT PARTICIPATION

If the operations director determines that Crisis Response Unit participation is appropriate, the director and the SWAT supervisor shall work together to develop a written plan. The SWAT supervisor shall assume operational control until the individuals at the scene are appropriately detained and it is safe to begin a search. When this occurs, the SWAT supervisor shall transfer control of the scene to the handling supervisor. This transfer should be communicated to the officers present.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Operations Planning and Deconfliction

614.8 MEDIA ACCESS

No advance information regarding the operation shall be released without the approval of the Chief of Police. Any media inquiries or press release after the fact shall be handled in accordance with the Media Relations Policy.

614.9 DEBRIEFING

As soon as reasonably practicable, the operation should be debriefed. The debriefing should include as many participants as possible. This debrief may be separate from any SWAT debriefing.

614.10 REPORTING REQUIREMENTS

A report shall be prepared for all reportable incidents in the format developed by the Commission on Criminal and Juvenile Justice (CCJJ), as required by Utah Code 77-7-8.5. This report including all reportable incidents which occurred in the prior year shall be submitted to the Chief of Police by February 1st of each year (see the Warrant Service Policy).

Reportable incidents include SWAT deployments for situations other than warrant service, such as hostage or barricaded subjects. This information should be obtained from the SWAT Commander.

The Chief of Police shall review and approve the report and ensure that it is forwarded to the CCJJ and the designated recipient for the City no later than April 30th.

614.11 TRAINING

Officers and SWAT team members who participate in these types of operations should receive periodic training on this policy, including, but not limited to, the following:

- Legal issues
- Deconfliction practices
- Warrant preparation
- Warrant service
- Operations plan preparation
- Reporting requirements

Warrant Service

615.1 PURPOSE AND SCOPE

This policy establishes guidelines for the planning and serving of arrest and search warrants by members of this Department. It is understood that this policy cannot address every variable or circumstance that can arise in the service of a search or arrest warrant, as these tasks can involve rapidly evolving and unique circumstances.

This policy is intended to be used in conjunction with the Operations Planning and Deconfliction Policy, which has additional guidance on planning and serving high-risk warrants.

This policy is not intended to address the service of search warrants on locations or property already secured or routine field warrant arrests by patrol officers.

615.1.1 DEFINITIONS

Definitions related to this policy include:

Reportable incident - An incident where forcible entry is used or a special unit specifically trained and equipped to respond to critical, high-risk situations is deployed in the service of a search warrant (Utah Code 77-7-8.5).

615.2 POLICY

It is the policy of the South Salt Lake Police Department to balance the safety needs of the public, the safety of department members, privacy interests and other relevant factors when making decisions related to the service of search and arrest warrants.

615.3 OPERATIONS DIRECTOR

The operations director (see the Operations Planning and Deconfliction Policy) shall review all risk assessment forms with the involved supervisor to determine the risk level of the warrant service.

The operations director will also have the responsibility to coordinate service of those warrants that are categorized as high risk. Deconfliction, risk assessment, operational planning, briefing and debriefing should follow guidelines in the Operations Planning and Deconfliction Policy.

615.3.1 REPORTING REQUIREMENTS

The operations director shall prepare a report on all reportable incidents in the format developed by the Commission on Criminal and Juvenile Justice (CCJJ), as required by Utah Code 77-7-8.5. The director shall ensure that reports on all reportable incidents in the prior year are submitted to the Chief of Police by February 1 of each year (see the Operations Planning and Deconfliction Policy for additional reporting requirements).

The Chief of Police shall review and approve the report and ensure that it is forwarded to the CCJJ and the designated recipient for the City no later than April 30.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Warrant Service

615.3.2 MODEL GUIDELINES OF THE UTAH PEACE OFFICER STANDARDS AND TRAINING COUNCIL

The operations director shall be familiar with any model guidelines and procedures recommended by the Utah Peace Officer Standards and Training Council regarding warrants and ensure members follow the guidelines and procedures (Utah Code 77-23-210).

615.4 SEARCH WARRANTS

Officers should receive authorization from a supervisor before preparing a search warrant application. Once authorization is received, the officer will prepare the affidavit and search warrant, consulting with the applicable prosecuting attorney as needed. He/she will also complete the risk assessment form and submit it, along with the warrant affidavit, to the appropriate supervisor and the operations director for review and classification of risk (see the Operations Planning and Deconfliction Policy).

615.5 ARREST WARRANTS

If an officer reasonably believes that serving an arrest warrant may pose a higher risk than commonly faced on a daily basis or require forcible entry onto the property or building where the person to be arrested is located, the officer should complete the risk assessment form and submit it to the appropriate supervisor and the operations director for review and classification of risk (Utah Code 77-7-8; Utah Code 77-7-8.1) (see the Operations Planning and Deconfliction Policy).

If the warrant is classified as high risk, service will be coordinated by the operations director. If the warrant is not classified as high risk, the supervisor should weigh the risk of entry into a residence to make an arrest against other alternatives, such as arresting the person outside the residence where circumstances may pose a lower risk.

615.6 WARRANT PREPARATION

An officer who prepares a warrant should ensure the documentation in support of the warrant contains as applicable:

- (a) Probable cause to support the search or arrest, including relevant dates and times to demonstrate timeliness and facts to support any request for nighttime or no-knock warrant execution.
 - 1. No-knock warrant applications shall be consistent with the requirements of state law (Utah Code 77-7-8.1).
- (b) A clear explanation of the affiant's training, experience, and relevant education.
- (c) Adequately supported opinions, when relevant, that are not left to unsubstantiated conclusions.
- (d) A nexus between the place to be searched and the persons or items central to the investigation. The facts supporting this nexus should be clear and current. For example, the affidavit shall explain why there is probable cause to believe that a particular person is currently residing at a particular location or that the items sought are present at a particular location.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Warrant Service

- (e) Full disclosure of known or suspected residents at the involved location and any indication of separate living spaces at the involved location. For example, it should be disclosed that several people may be renting bedrooms at a single location, even if the exact location of the rooms is not known.
- (f) A specific description of the location to be searched, including photographs of the location, if reasonably available.
- (g) A sufficient description of the items to be seized.
- (h) Full disclosure of any known exculpatory information relevant to the warrant application (refer to the *Brady* Material Disclosure Policy).

615.7 HIGH-RISK WARRANT SERVICE

The operations director or the authorized designee shall coordinate the service of warrants that are categorized as high risk and shall have sole authority in determining the manner in which the warrant will be served, including the number of officers deployed.

The member responsible for directing the service should ensure the following as applicable:

- (a) When practicable and when doing so does not cause unreasonable risk, video or photographic documentation is made of the condition of the location prior to execution of a search warrant. The images should include the surrounding area and persons present.
- (b) The warrant service is audio- and video-recorded when practicable and reasonable to do so.
 - 1. Members executing a warrant shall wear a body-worn camera unless exigent circumstances make the use of such camera impracticable (Utah Code 77-23-210).
- (c) Evidence is handled and collected only by those members who are designated to do so. All other members involved in the service of the warrant should alert one of the designated members to the presence of potential evidence and not touch or disturb the items.
- (d) Reasonable efforts are made during the search to maintain or restore the condition of the location.
- (e) Persons who are detained as part of the warrant service are handled appropriately under the circumstances.
- (f) Reasonable care provisions are made for children and dependent adults (see the Child and Dependent Adult Safety Policy).
- (g) A list is made of all items seized and a copy provided to the person in charge of the premises if present or otherwise left in a conspicuous place.
- (h) A copy of the search warrant is left at the location.
- (i) The condition of the property is documented with video recording or photographs after the search.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Warrant Service

- (j) Absent exigent circumstances, officers serving a search warrant shall wear a uniform or other clothing that clearly identifies them as law enforcement, including a badge and law enforcement label (Utah Code 77-23-210; Utah Code 77-7-8; Utah Code 77-7-8.1).

615.8 DETENTIONS DURING WARRANT SERVICE

Officers must be sensitive to the safety risks of all persons involved with the service of a warrant. Depending on circumstances and facts present, it may be appropriate to control movements of any or all persons present at a warrant service, including those who may not be the subject of a warrant or suspected in the case. However, officers must be mindful that only reasonable force may be used and weapons should be displayed no longer than the officer reasonably believes is necessary (see the Use of Force Policy).

As soon as it can be determined that an individual is not subject to the scope of a warrant and that no further reasonable suspicion or safety concerns exist to justify further detention, the person should be promptly released.

Officers should, when and to the extent reasonable, accommodate the privacy and personal needs of people who have been detained.

615.9 ACTIONS AFTER WARRANT SERVICE

The supervisor shall ensure that all affidavits, warrants, receipts and returns, regardless of any associated cases, are filed with the issuing judge or magistrate as soon as reasonably possible, but in any event no later than any date specified on the warrant.

615.9.1 NOTIFICATIONS REGARDING USE OF IMAGING SURVEILLANCE DEVICE

When an imaging surveillance device is used during the service of a warrant, notification shall be made to the person who owns or otherwise resides at the location specified in the warrant within 14 days unless a court-ordered extension has been granted (Utah Code 77-23d-104).

615.10 OUTSIDE AGENCIES AND CROSS-JURISDICTIONAL WARRANTS

The operations director will ensure that cooperative efforts with other agencies in the service of warrants conform to existing mutual aid agreements or other memorandums of understanding and will work cooperatively to mitigate risks including, but not limited to, the following:

- Identity of team members
- Roles and responsibilities
- Familiarity with equipment
- Rules of engagement
- Asset forfeiture procedures

Any outside agency requesting assistance in the service of a warrant within this jurisdiction should be referred to the operations director. The director should review and confirm the warrant, including the warrant location, and should discuss the service with the appropriate supervisor from the other agency. The director should ensure that members of the South Salt Lake Police Department

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Warrant Service

are utilized appropriately. Any concerns regarding the requested use of South Salt Lake Police Department members should be brought to the attention of the Chief of Police or the authorized designee. The actual service of the warrant will remain the responsibility of the agency requesting assistance.

If the operations director is unavailable, the Watch Commander should assume this role.

If officers intend to serve a warrant outside South Salt Lake Police Department jurisdiction, the operations director should provide reasonable advance notice to the applicable agency, request assistance as needed, and work cooperatively on operational planning and the mitigation of risks detailed in this policy.

Officers will remain subject to the policies of the South Salt Lake Police Department when assisting outside agencies or serving a warrant outside the South Salt Lake Police Department jurisdiction.

615.11 MEDIA ACCESS

No advance information regarding warrant service operations shall be released without the approval of the Chief of Police. Any media inquiries or press release after the fact shall be handled in accordance with the Media Relations Policy.

615.12 TRAINING

The Training Coordinator should ensure officers receive periodic training on this policy and associated topics, such as legal issues, warrant preparation, warrant service, and reporting requirements.

615.13 NO-KNOCK ENTRIES

No-knock entries are only authorized if a no-knock warrant has been obtained in accordance with Utah Code 77-7-8.1 or Utah Code 77-23-210 or if exigent circumstances arise at the scene such that knocking and announcing the officer's presence would create an imminent threat of physical violence to the officer or another person.

615.14 DOCUMENTATION

Documentation related to the service of a warrant shall be maintained in accordance with the established records retention schedule.

Investigative Genetic Genealogy

616.1 PURPOSE AND SCOPE

This policy provides guidance for the use of investigative genetic genealogy (IGG) to generate investigative leads.

616.1.1 DEFINITIONS

Definitions related to this policy include:

Combined DNA Index System (CODIS) - An FBI computer software program that operates deoxyribonucleic acid (DNA) profile databases for law enforcement use.

DNA typing laboratory - A laboratory that analyzes biological samples, including extracted DNA, in order to provide various DNA profile types. State or local crime labs are generally not equipped to provide single nucleotide polymorphisms (SNP) DNA profiles; therefore, the use of private DNA typing laboratories is often necessary for IGG.

Extracted DNA - The DNA isolated from a biological sample remaining after previous DNA testing has been completed.

Genetic genealogist - A genealogist who uses DNA testing with traditional genealogical research methods to assist law enforcement or private clients in identifying biological relatives of an individual.

Genetic genealogy site - A database of DNA profiles voluntarily submitted by public consumers for the purpose of identifying genetic relatives. The availability of genetic genealogy sites for law enforcement use varies depending on their terms of service.

Investigative genetic genealogy (IGG) - The process of obtaining a SNP DNA profile from a biological sample collected during an investigation; uploading the profile to a genetic genealogy site for comparison to the consumer profiles in the site's database to identify genetic relatives; and using the identified genetic relationships, as well as traditional genealogy research, to generate investigative leads.

Short tandem repeat (STR) DNA profile - The results of DNA typing in a format that can be processed through CODIS and state DNA databases. This is the type of DNA used in conventional non-IGG law enforcement investigations.

Single nucleotide polymorphism (SNP) DNA profile - The results of DNA typing in a format that enables an unknown DNA sample to be compared to the DNA profiles maintained by a genetic genealogy site. This is the DNA type used in IGG.

616.2 POLICY

The South Salt Lake Police Department's use of IGG will be in coordination with prosecutors, the [Medical Examiner/JOP], and other appropriate resources only in qualifying cases after reasonable conventional investigative methods have been pursued. Members will take reasonable steps to

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Investigative Genetic Genealogy

maintain the integrity of the IGG process and safeguard the privacy rights of individuals whose DNA profiles are analyzed.

616.3 CRITERIA FOR IGG USE

Before using IGG, the lead investigator should coordinate with the supervisor to determine whether the case meets the following requirements (Utah Code 53-10-403.7):

- (a) Biological evidence collected as part of the underlying investigation (or extracted DNA from the biological evidence) of a qualifying case is available for additional testing and is reasonably believed to be attributable to:
 - 1. The perpetrator of an unsolved violent felony.
 - 2. Unidentified human remains.
 - 3. A missing or unknown individual.
- (b) All reasonable conventional investigative methods have been utilized and all reasonable investigative leads have been pursued (e.g., relevant case information entered in the National Missing and Unidentified Persons System (NamUs) and the Violent Criminal Apprehension Program (ViCAP) national database).
- (c) An STR DNA profile has been developed from the biological evidence collected in the case and, absent unusual circumstances, has been uploaded to CODIS and any applicable state DNA database for comparison with negative results.

616.4 COORDINATION

Once a preliminary determination has been made that a case may qualify for the use of IGG, the lead investigating member should consult with the appropriate prosecutor to address current and prospective legal issues and determine if a search warrant is required.

In the case of unidentified human remains, the lead investigator should also consult with the [MedicalExaminer/JOP].

616.4.1 CONSULTATION WITH PROSECUTOR AND BUREAU OF FORENSIC SERVICE

The lead investigating member shall consult with the prosecuting attorney and the Bureau of Forensic Services to determine whether IGG is appropriate and necessary before proceeding with IGG. The [Department/Office] and the prosecuting agency shall agree to investigate relevant leads resulting from IGG (Utah Code 53-10-403.7).

616.5 SUBMISSION OF SAMPLE

The biological evidence or extracted DNA should be submitted to a DNA typing laboratory approved by the [Department/Office] in order to obtain a SNP DNA profile.

Once a SNP DNA profile has been obtained from the biological evidence or extracted DNA, the lead investigating member should arrange for it to be compared to the SNP DNA profiles contained in one or more genetic genealogy sites to identify possible genetic relatives. The lead investigator should work with a qualified genetic genealogist as needed during this process.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Investigative Genetic Genealogy

When submitting a SNP DNA profile for comparison, the lead investigator or the authorized designee (e.g., assigned genetic genealogist) shall notify the genetic genealogy site that the request for comparison is from a law enforcement agency and confirm that the site's terms of service permit IGG for the type of case being investigated (Utah Code 53-10-403.7). The use of the SNP DNA profile and any subsequent comparison shall be limited to the original underlying investigation.

If at any time during the IGG process the case no longer meets the criteria for IGG use, the lead investigator should promptly notify the DNA typing laboratory, genetic genealogy site, and/or genetic genealogist to cease any further analysis and to return all evidence, data, and materials to the [Department/Office].

616.5.1 ADDITIONAL REQUIREMENTS FOR SUBMISSION

The lead investigator shall take steps to restrict IGG to genetic genealogy sites that provide appropriate notice to their users of possible law enforcement use, allow users to opt-out of having their data accessible to law enforcement, and have policies to prevent third-party access to the data concerning a victim, crime scene, or suspect (Utah Code 53-10-403.7).

616.6 ANALYSIS OF IGG DATA

Once results of a comparison are received from a genetic genealogy site, the information should be evaluated by a genetic genealogist, who will assist the lead investigator in identifying potential investigative leads.

The lead investigator should promptly and diligently pursue each viable lead identified through the IGG process using traditional investigative methods, as appropriate, to:

- (a) Eliminate an individual as a potential suspect in the case.
- (b) Link an individual to the case as a potential suspect.
- (c) Identify human remains.

616.7 COLLECTION OF THIRD-PARTY DNA SAMPLE

If it is determined that a third-party DNA sample (i.e., from a person not likely to be a suspect in the investigation) should be collected and analyzed for IGG, consent from the third party should be obtained prior to collection (Utah Code 53-10-403.7).

If there is a reasonable belief that the integrity of the investigation would be compromised by seeking consent from the third party prior to collection, the lead investigator should consult with the prosecutor regarding applicable laws and procedures in both the jurisdiction of the investigation and the jurisdiction where the collection will occur, if different (Utah Code 53-10-403.7).

The use of a third-party DNA sample shall be limited to the original underlying investigation.

616.8 POST-IDENTIFICATION

Members shall not rely solely on IGG identification of a potential suspect for probable cause to make an arrest or obtain an arrest warrant. Unless there is sufficient evidence independent of the

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Investigative Genetic Genealogy

IGG data to support an arrest, a potential suspect identified through IGG should not be arrested until the suspect's identity is confirmed (Utah Code 53-10-403.7).

Members shall not rely solely on IGG to identify human remains unless there is sufficient evidence independent of the IGG data to declare the identification or confirmation testing has been completed.

Confirmatory DNA testing should be conducted by collecting a known DNA sample from the potential suspect or, in the case of unidentified human remains, from a close biological relative. This known DNA sample should be submitted for comparison to the original unknown STR DNA profile through conventional methods (e.g., in CODIS).

The lead investigator should consult with the prosecutor to determine the appropriate method of obtaining a known DNA sample.

Once the identity of a suspect or the identity of unidentified human remains has been confirmed through conventional DNA testing, the lead investigator should:

- (a) Consult with the prosecutor to evaluate the entire investigative file for consideration of criminal charges or further investigation.
- (b) If applicable, consult with the [MedicalExaminer/JOP] for an amendment to a certificate of death.

616.9 PRIVACY CONSIDERATIONS

Members should make reasonable efforts to respect and protect the privacy of non-suspect genetic relatives identified through the IGG process. The names and identifying information of any non-suspect genetic relatives should not be included in official reports, probable cause declarations, or affidavits for search warrants and should not be disclosed unless otherwise required by law or court order.

The lead investigator should formally request that the SNP DNA profile be removed from all genetic genealogy sites upon identity confirmation and should retain a copy of the request for [department/office] records (Utah Code 53-10-403.7). The lead investigator should request that all case-related records and data provided to, or generated by, a genetic genealogist during the IGG process be returned to the [Department/Office].

616.10 RETENTION OF DNA SAMPLES AND RELATED RECORDS

Genetic information, including any derivative profiles and genetic genealogy site user information, should be retained for the minimum period established by law and destroyed once permitted by Utah law (Utah Code 53-10-403.7). The lead investigator should coordinate with the property and evidence technician and provide adequate notice to the appropriate prosecutor's office before destroying any profiles or data obtained from the IGG process.

See the Property and Evidence Policy for guidelines regarding biological evidence, including DNA samples.

Facial Recognition Technology Use

617.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the use of facial recognition technology (FRT) by the [Department/Office] to assist in the development of investigative leads. This policy also provides guidance for FRT data access, use, and retention.

This policy does not apply to the use of FRT in user identification applications for personal electronic devices, access control systems, or automated video redaction software.

617.1.1 DEFINITIONS

Definitions related to this policy include:

Biometric surveillance information - Information obtained through the digital monitoring of an area that is analyzed using FRT to determine an individual's identity or location based on their physical attributes or manner. (Utah Code § 77-23d-102).

Facial recognition technology (FRT) - A software application, electronic system, or a third-party service that uses biometric algorithms to compare facial features of a probe image with the features of images contained within an image database.

Government image database – A database maintained by the [Department/Office] or another government entity of images captured during interactions with the [Department/Office] or government entity. This does not include publicly available information (Utah Code 77-23e-102).

Probe image - A search image submitted to FRT for comparison with images contained within an image database.

617.2 POLICY

It is the policy of the South Salt Lake Police Department to limit FRT use to developing investigative leads for legitimate law enforcement purposes while recognizing and protecting established constitutional and privacy rights.

617.3 CHIEF OF POLICE RESPONSIBILITIES

The Chief of Police or the authorized designee shall approve any FRT system or service prior to its implementation and use by the [Department/Office].

617.4 FRT COORDINATOR

The Chief of Police or the authorized designee shall appoint an FRT coordinator. The responsibilities of the FRT coordinator include:

- (a) Establishing procedures for [department/office] FRT use that conform to applicable laws, regulations, and best practices. Procedures should include:
 - 1. A process for submitting and assessing officer requests to use FRT.
 - 2. Requirements related to processing and reviewing results generated from the use of FRT.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Facial Recognition Technology Use

3. Requirements for complying with Utah Code 77-23e-105 prior to implementing new FRT systems (i.e., posting proper notice, accepting and reviewing public comments, posting final decisions).
- (b) Establishing procedures for collecting, processing, and storing FRT data.
 1. Procedures should include the management of biometric surveillance information (Utah Code 77-23d-106).
- (c) Establishing procedures for access and security controls for [department/office] FRT systems, services, and data.
 1. Access levels should be no higher than necessary to accomplish organizational tasks, missions, or functions.
- (d) Establishing procedures for submitting images to [department/office] image databases. The procedures should include:
 1. When and under what circumstances members are required to submit images.
 2. Restrictions related to the use of images voluntarily provided to the [Department/Office] by members of the public.
- (e) Administering data quality assurance measures (e.g., probe image suitability, quality, integrity).
- (f) Conducting periodic audits of [department/office] FRT use.
 1. The audit should include a review of FRT use, documentation of those uses, and confirmation of data purging, where appropriate.
 2. The audit should include a review of the use of biometric surveillance information (Utah Code 77-23d-106).
- (g) Confirming that authorized users have completed [department/office]-approved FRT and forensic image comparison training prior to using FRT.
- (h) Coordinating with the Training Coordinator to develop, identify, and update FRT training for officers who utilize the FRT system.
- (i) Establishing and implementing a schedule for routine maintenance, upgrades, enhancements, testing, and refreshes of FRT for proper performance purposes.
- (j) Establishing procedures for reporting errors, malfunctions, or deficiencies of FRT systems, services, or data.
- (k) Coordinating with the information systems technology supervisor, [department/office] counsel, and appropriate administrators to develop information-sharing procedures with outside agencies in accordance with state and federal law.
- (l) Evaluating systems to verify that, in accordance with industry standards, FRT used on a government image database managed by the [Department/Office] is secure, produced by a company that is currently in business, and makes comparisons using an algorithm that compares only facial biometric data (Utah Code 77-23e-103).
- (m) Ensuring this policy is posted and publicly available on the [department/office] website or the Utah Public Notice Website, as applicable (Utah Code 77-23d-106).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Facial Recognition Technology Use

617.5 AUTHORIZED USES OF FRT

FRT may be used as a tool to develop investigative leads for legitimate law enforcement purposes to assist in the identification of the following:

- (a) Unknown suspects where attempts at identification through other means have been exhausted or ineffective
- (b) Potential victims, as appropriate (e.g., human trafficking, child sexual abuse material)
- (c) Deceased individuals
- (d) Individuals who are incapacitated or do not know their identities
- (e) Individuals who are lawfully detained and whose identities are in question (e.g., no identification or false identification provided)
- (f) Suspects in unsolved crimes
- (g) Missing or endangered persons
- (h) Unknown individuals pursuant to any other legitimate law enforcement purpose

617.5.1 AUTHORIZED USES OF FRT ON GOVERNMENT IMAGE DATABASE

FRT shall only be used on a government image database for the following purposes (Utah Code 77-23e-103):

- (a) Investigating a felony, a violent crime, or a threat to human life
- (b) Identifying an individual who is:
 - 1. Deceased.
 - 2. Incapacitated.
 - 3. At risk and otherwise unable to provide their identity.

617.6 REQUEST FOR AUTHORIZATION

An officer seeking authorization to conduct or request an FRT search shall submit a request to the appropriate supervisor consistent with [department/office] procedures.

The request should, at a minimum, include the following:

- (a) The nature of the investigation
- (b) The reason an officer believes that FRT use is necessary
- (c) An explanation of how FRT may assist with the development of investigative leads
- (d) A case identification number

617.7 FRT SEARCHES

Following supervisor approval, the officer should proceed as follows:

- (a) An officer seeking to have a probe image compared to images contained in a government image database shall submit the probe image and a written FRT request to a member of this [department/office] who is trained and authorized to conduct FRT

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Facial Recognition Technology Use

searches or to the government entity that maintains the database, as appropriate (Utah Code 77-23e-103).

- (b) An officer seeking to have a probe image compared to images contained in a database maintained by the Department of Public Safety shall submit the probe image and FRT request through the Utah Criminal Justice Information System (Utah Code 77-23e-104).
- (c) For all other FRT use, an officer should submit a probe image for comparison consistent with [department/office] procedures.
- (d) Officers shall only submit lawfully obtained probe images.

Only members authorized by the [Department/Office] may conduct FRT searches. Before proceeding with official law enforcement action based on FRT results, the results should be thoroughly reviewed by a member trained in FRT.

617.7.1 FRT SEARCH OF GOVERNMENT DATABASE

An FRT search on a government image database maintained by the [Department/Office] shall only be conducted upon receipt of a written request from an officer of this [department/office] or from another law enforcement agency. The request shall include (Utah Code 77-23e-103):

- (a) The authorized purpose for which the request is made.
- (b) The case identification number.
- (c) If applicable, a statement of the specific crime being investigated and a factual narrative to support that there is a fair probability that the individual who is the subject of the request is connected to the crime.

Before providing results to the requesting officer or entity, the results should be verified and reviewed according to Utah Code 77-23e-103. No search results other than a probable match agreed upon by at least two authorized members shall be provided in response to a request for FRT (Utah Code 77-23e-103).

617.7.2 USES AND LIMITATIONS OF FRT SEARCH RESULTS

Information resulting from an FRT search shall be considered an investigative lead only and not a positive identification of any person or utilized solely as the basis for engaging in any law enforcement action. Image comparisons generated from FRT use do not represent definitive confirmation of an identity match or non-match. Any positive identification and connection of a person to an investigation shall be determined through additional investigative means and resources.

617.7.3 FRT SEARCH DOCUMENTATION

The investigating officer shall document all FRT searches in the appropriate [department/office] report, including any arrest report where FRT was used as an investigative tool. Documentation shall include:

- (a) The requesting officer's name and position.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Facial Recognition Technology Use

- (b) Confirmation that the search was pre-approved pursuant to [department/office] procedures.
- (c) The purpose of the search.
- (d) The search parameters, if any.
- (e) The date and time of the search.
- (f) A list of any image databases searched.
- (g) The results of the search, including the number of investigative leads produced and, where applicable, the matching score of each.
 - 1. This includes information received indicating an FRT search produced no results (Utah Code 77-23e-103).
- (h) The additional means used to identify any person (e.g., visual comparison of images by a trained investigator, other subsequent investigation).
- (i) A description of how the facial recognition comparison was used in the investigation (Utah Code 77-23e-103).

617.8 PRIVACY CONSIDERATIONS

The [Department/Office] shall adhere to all applicable federal and state laws regarding privacy concerns related to FRT use. Officers shall take reasonable precautions to avoid inadvertently recording or capturing images where there is a reasonable expectation of privacy.

617.8.1 NOTICE OF POTENTIAL FRT USE

When capturing an image of an individual during an interaction with the [department/office], the individual shall be notified that their image may be used in conjunction with FRT (Utah Code 77-23e-105).

617.8.2 BIOMETRIC SURVEILLANCE INFORMATION

Biometric surveillance information shall only be obtained as follows (Utah Code 77-23d-106):

- (a) In accordance with a search warrant.
- (b) On authorized property, as defined by Utah Code 77-23d-102.
- (c) In accordance with a judicially recognized exception to warrant requirements.
- (d) When there is a documented reasonable articulable suspicion that a specific individual has threatened to commit a violent felony toward a person, group of people, or place, or to commit an offense of threat of violence under Utah Code 76-5-107.

617.9 PROHIBITED USES

FRT shall not be used in a manner that targets individuals or groups solely based on actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, age, disability, or any other classification or status protected by law.

In addition, FRT shall not be used:

- (a) For the arrest of individuals based solely on FRT results.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Facial Recognition Technology Use

- (b) For any purpose that violates the U.S. Constitution or laws of the United States, including the protections of the First, Fourth, and 14th Amendments.
- (c) For any non-law enforcement purpose.
- (d) As the sole basis for identification to establish probable cause in a criminal investigation.
- (e) To harass or intimidate any individual or group.
- (f) In any other manner that would violate applicable law, regulation, or policy.
- (g) On a government image database to investigate civil immigration violations (Utah Code 77-23e-103).

No officer shall request that a third-party use FRT to obtain results that would not be permitted under this policy.

617.10 RELEASE OF FRT DATA

Data related to FRT use on a government image database is not subject to the Government Records Access and Management Act and shall not be disclosed except as required by law or court order (Utah Code 77-23e-106).

All other FRT data should only be released to the public in accordance with federal and state public record laws. Requests for the release of FRT data shall be processed in accordance with the Records Maintenance and Release Policy.

617.11 RETENTION OF FRT DATA

FRT data shall be retained in accordance with the established records retention schedule.

Unmatched probe images shall be purged in accordance with the established records retention schedule.

617.12 DOCUMENTATION

Members conducting FRT searches on a government image database maintained by the [Department/Office] should document FRT data in a way that facilitates statistical reporting required by Utah Code 77-23e-106 (see the Records Section Policy).

617.13 TRAINING

Officers whose duties may require the use of FRT should receive initial training and periodic refresher training on this policy and related procedures and should demonstrate their knowledge and understanding. Training should include but is not limited to the following (Utah Code 77-23e-102):

- (a) Capabilities and limitations of FRT
- (b) FRT system functions and interpretation of results
- (c) Data security and privacy concerns
- (d) Documentation and reporting requirements (e.g., FRT results, general statistics, collection of FRT data, FRT requests)

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Facial Recognition Technology Use

- (e) Digital media handling and protections
- (f) Common terminology (e.g., human face recognition, automated face recognition, holistic face processing, unfamiliar face matching)
- (g) Principles of comparison
- (h) Cognitive bias, confirmation bias, implicit bias, and automation bias
- (i) Applicable policy, procedure, and federal and state law requirements

An officer who uses mobile facial recognition shall receive additional training appropriate to that application of the technology.

The FRT coordinator shall maintain a record of each authorized officer's training and acknowledgement of this policy.

Chapter 7 - Equipment

Department Owned and Personal Property

700.1 PURPOSE AND SCOPE

This policy addresses the care of [department/office]-owned property and the role of the [Department/Office] when personal property, the property of another, or [department/office]-owned property is damaged or lost.

700.2 DAMAGE TO PROPERTY OF ANOTHER PERSON OR ENTITY

Members who intentionally or unintentionally damage or cause to be damaged the real or personal property of another person or entity while performing any law enforcement function shall promptly report the damage through the member's chain of command.

700.2.1 DAMAGE BY PERSONNEL OF ANOTHER AGENCY

Personnel from another agency may intentionally or unintentionally cause damage to the real or personal property of the City of South Salt Lake or of another person while performing their duties within the jurisdiction of this [department/office]. The [department/office] member present or the member responsible for the property is responsible to report the damage as follows:

- (a) A verbal report shall be made to the member's immediate supervisor as soon as circumstances permit.
- (b) A written report shall be submitted before the member goes off-duty or as otherwise directed by the supervisor.

700.3 POLICY

The South Salt Lake Police Department will ensure that members are issued appropriate property and equipment necessary for the member's job function. The [Department/Office] will take steps to minimize the cost associated with maintaining [department/office] property, including personal property authorized for use in the member's duties.

700.4 SUPERVISOR RESPONSIBILITIES

The supervisor receiving a report that property, including personal property authorized for use, has been damaged should conduct an investigation and direct a memo to the appropriate Division Commander. The memo should include the result of the investigation and whether reasonable care was taken to prevent the loss, damage, or unserviceable condition.

Cases where the supervisor has reason to believe that misconduct or negligence was involved in the loss, damage, or unserviceable condition of property should be handled in accordance with the Standards of Conduct and Personnel Complaints policies.

700.5 DEPARTMENT ISSUED PROPERTY

The Administration supervisor should document all property and equipment issued by the [Department/Office] in the appropriate file at the time of issuance. Receipt of issued items shall be acknowledged by the receiving member's signature. Upon separation from the [Department/

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Department Owned and Personal Property

Office], all issued property and equipment shall be returned. Documentation of the return shall be acknowledged by the signature of a supervisor.

700.5.1 MEMBER RESPONSIBILITIES

Members shall be responsible for the safekeeping, serviceable condition, proper care, proper use, and replacement of [department/office]-issued property that has been assigned or entrusted to them.

- (a) Members shall promptly report, through their chain of command, the loss, damage, or unserviceable condition of any [department/office]-issued property or equipment.
- (b) The use of damaged or unserviceable property should be discontinued as soon as practicable, and the item replaced with a comparable item as soon as available.
- (c) Except when otherwise directed by a supervisor or when exigent circumstances exist, [department/office]-issued property shall only be used by those to whom it was assigned. Use should be limited to official purposes and in the capacity for which it was designed.
- (d) [Department/Office]-issued property shall not be thrown away, sold, traded, donated, destroyed, or otherwise disposed of without prior approval.
- (e) Members should obtain a supervisor's approval before any attempt to repair damaged or unserviceable property, unless the repair is of a minor or temporary nature.

700.6 PERSONAL PROPERTY

Carrying and/or using personal property or equipment on-duty requires prior written approval by the Chief of Police or designee.. The member should submit a request that includes a description of the property and the reason and length of time it will be used. Personal property of the type routinely carried by persons who are not performing law enforcement duties, and that is not a weapon, is excluded from this requirement.

The [Department/Office] will not replace or repair items (e.g., jewelry, expensive watches) that are not reasonably required as part of work.

700.6.1 FILING CLAIMS FOR PERSONAL PROPERTY

A member requesting reimbursement for damage to, or loss of, personal property must submit the request in writing to the member's immediate supervisor. The supervisor may require a separate written report.

Upon review by command staff and a finding that no misconduct or negligence was involved, repair or replacement may be recommended by the Chief of Police, who will then forward the claim to the City department responsible for issuing payments.

Information Technology Use

701.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the proper use of [department/office] information technology resources, including computers, electronic devices, hardware, software, and systems.

701.1.1 DEFINITIONS

Definitions related to this policy include:

Computer system - All computers (on-site and portable), electronic devices, hardware, software, and resources owned, leased, rented, or licensed by the South Salt Lake Police Department that are provided for official use by its members. This includes all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the [Department/Office] or [department/office] funding.

Hardware - Includes but is not limited to computers, computer terminals, network equipment, electronic devices, telephones, including cellular and satellite, modems, or any other tangible computer device generally understood to comprise hardware.

Software - Includes but is not limited to all computer programs, systems, and applications, including shareware and firmware. This does not include files created by the individual user.

Temporary file, permanent file, or file - Any electronic document, information, or data residing or located, in whole or in part, on the system including but not limited to spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, messages, photographs, or videos.

701.2 POLICY

It is the policy of the South Salt Lake Police Department that members shall use information technology resources, including computers, software, and systems, that are issued or maintained by the [Department/Office] in a professional manner and in accordance with this policy.

701.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to emails, texts, or anything published, shared, transmitted, or maintained through file-sharing software or any internet site that is accessed, transmitted, received, or reviewed on any [department/office] computer system.

The [Department/Office] reserves the right to access, audit, and disclose, for whatever reason, any message, including attachments, and any information accessed, transmitted, received, or reviewed over any technology that is issued or maintained by the [Department/Office], including the [department/office] email system, computer network, and/or any information placed into storage on any [department/office] system or device. This includes records of all keystrokes or web-browsing history made at any [department/office] computer or over any [department/office] network. The fact that access to a database, service, or website requires a username or password

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Information Technology Use

will not create an expectation of privacy if it is accessed through [department/office] computers, electronic devices, or networks.

The [Department/Office] may not require a member to disclose a username and/or password that allows access to the member's personal internet accounts, except as may be provided in Utah Code 34-48-201.

701.4 RESTRICTED USE

Members shall not access computers, devices, software or systems for which they have not received prior authorization or the required training. Members shall immediately report unauthorized access or use of computers, devices, software or systems by another member to their supervisors or Watch Commanders.

Members shall not use another person's access passwords, logon information and other individual security data, protocols and procedures unless directed to do so by a supervisor.

701.4.1 SOFTWARE

Members shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes in accordance with the software company's copyright and license agreement.

To reduce the risk of a computer virus or malicious software, members shall not install any unlicensed or unauthorized software on any [department/office] computer. Members shall not install personal copies of any software onto any [department/office] computer.

When related to criminal investigations, software program files may be downloaded only with the approval of the information systems technology (IT) staff and with the authorization of the Chief of Police or the authorized designee.

No member shall knowingly make, acquire, or use unauthorized copies of computer software that is not licensed to the [Department/Office] while on [department/office] premises, computer systems, or electronic devices. Such unauthorized use of software exposes the [Department/Office] and involved members to severe civil and criminal penalties.

Introduction of software by members should only occur as part of the automated maintenance or update process of [department/office]- or City-approved or installed programs by the original manufacturer, producer, or developer of the software.

Any other introduction of software requires prior authorization from IT staff and a full scan for malicious attachments.

701.4.2 HARDWARE

Access to technology resources provided by or through the [Department/Office] shall be strictly limited to [department/office]-related activities. Data stored on or available through [department/office] computer systems shall only be accessed by authorized members who are engaged in an active investigation or assisting in an active investigation, or who otherwise have a legitimate law enforcement or [department/office]-related purpose to access such data. Any exceptions to this policy must be approved by a supervisor.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Information Technology Use

701.4.3 INTERNET USE

Internet access provided by or through the [Department/Office] shall be strictly limited to [department/office]-related activities. Internet sites containing information that is not appropriate or applicable to [department/office] use and which shall not be intentionally accessed include but are not limited to adult forums, pornography, gambling, chat rooms, and similar or related internet sites. Certain exceptions may be permitted with the express approval of a supervisor as a function of a member's assignment.

Downloaded information from the internet shall be limited to messages, mail, and data files.

701.4.4 OFF-DUTY USE

Members shall only use technology resources provided by the [Department/Office] while on-duty or in conjunction with specific on-call assignments unless specifically authorized by a supervisor. This includes the use of telephones, cell phones, texting, email, or any other "off the clock" work-related activities. This also applies to personally owned devices that are used to access [department/office] resources.

Refer to the Personal Communication Devices Policy for guidelines regarding off-duty use of personally owned technology.

701.5 PROTECTION OF SYSTEMS AND FILES

All members have a duty to protect the computer system and related systems and devices from physical and environmental damage and are responsible for the correct use, operation, care, and maintenance of the computer system.

Members shall ensure [department/office] computers and access terminals are not viewable by persons who are not authorized users. Computers and terminals should be secured, users logged off, and password protections enabled whenever the user is not present. Access passwords, logon information, and other individual security data, protocols, and procedures are confidential information and are not to be shared. Password length, format, structure, and content shall meet the prescribed standards required by the computer system or as directed by a supervisor and shall be changed at intervals as directed by IT staff or a supervisor. Passwords for accounts that access Criminal Justice Information (CJI) are governed by the CJIS Access, Maintenance, and Security Policy.

It is prohibited for a member to allow an unauthorized user to access the computer system at any time or for any reason. Members shall promptly report any unauthorized access to the computer system or suspected intrusion from outside sources (including the internet) to a supervisor.

701.6 INSPECTION OR REVIEW

A supervisor or the authorized designee has the express authority to inspect or review the computer system, all temporary or permanent files, related electronic systems or devices, and any contents thereof, whether such inspection or review is in the ordinary course of their supervisory duties or based on cause.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Information Technology Use

Reasons for inspection or review may include but are not limited to computer system malfunctions, problems or general computer system failure, a lawsuit against the [Department/Office] involving one of its members or a member's duties, an alleged or suspected violation of any [department/office] policy, a request for disclosure of data, or a need to perform or provide a service.

The IT staff may extract download, or otherwise obtain any and all temporary or permanent files residing or located in or on the [department/office] computer system when requested by a supervisor or during the course of regular duties that require such information.

Personal Communication Devices

702.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the use of mobile telephones and communication devices, whether issued or funded by the [Department/Office] or personally owned, while on-duty or when used for authorized work-related purposes.

This policy generically refers to all such devices as Personal Communication Devices (PCDs) but is intended to include all mobile telephones, personal digital assistants (PDAs), wireless-capable tablets, and similar wireless two-way communications and/or portable internet-access devices. PCD use includes but is not limited to placing and receiving calls, text messaging, blogging and microblogging, emailing, using video or camera features, playing games, and accessing sites or services on the internet.

702.2 POLICY

The South Salt Lake Police Department allows members to utilize [department/office]-issued or funded PCDs and to possess personally owned PCDs in the workplace, subject to certain limitations. Any PCD used while on- or off-duty for business-related purposes, or reasonably associated with work-related misconduct, will be subject to monitoring and inspection consistent with applicable law and this policy.

Additionally, the use of a PCD either on-duty or after duty hours for business-related purposes, or reasonably associated with work-related misconduct, may subject the member and the member's PCD records to civil or criminal discovery or disclosure under applicable public records laws.

Members who have questions regarding the application of this policy or the guidelines contained herein are encouraged to seek clarification from supervisory staff.

702.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to any communication accessed, transmitted, received, or reviewed on any PCD issued or funded by the [Department/Office] and shall have no expectation of privacy in their location should the device be equipped with location-detection capabilities. This includes records of all keystrokes or web-browsing history made on the PCD. The fact that access to a database, service, or website requires a username or password will not create an expectation of privacy if it is accessed through [department/office] PCDs or networks (see the Information Technology Use Policy for additional guidance).

Members have no expectation of privacy regarding any communications while using a personally owned PCD for [department/office]-related business or when the use reasonably implicates work-related misconduct.

702.4 DEPARTMENT/OFFICE-ISSUED PCD

Depending on a member's assignment and the needs of the position, the [Department/Office] may, at its discretion, issue or fund a PCD for the member's use to facilitate on-duty performance. [Department/Office]-issued or funded PCDs may not be used for personal business either on- or

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personal Communication Devices

off-duty unless authorized by the [agencyHead] or the authorized designee. Such devices and the associated telephone number, if any, shall remain the sole property of the [Department/Office] and shall be subject to inspection or monitoring (including all related records and content) at any time without notice and without cause.

Unless a member is expressly authorized by the Chief of Police or the authorized designee for off-duty use of the PCD, the PCD will be either secured in the workplace at the completion of the tour of duty or turned off when leaving the workplace.

702.5 PERSONALLY OWNED PCD

Members may carry a personally owned PCD while on-duty, subject to the following conditions and limitations:

- (a) Permission to carry a personally owned PCD may be revoked if it is used contrary to provisions of this policy.
- (b) The [Department/Office] accepts no responsibility for loss of or damage to a personally owned PCD.
- (c) The PCD and any associated services shall be purchased, used, and maintained solely at the member's expense.
- (d) The device should not be used for work-related purposes except in exigent circumstances (e.g., unavailability of radio communications) or as otherwise authorized by [department/office] procedures.
 - 1. Use of a personally owned PCD for work-related business constitutes consent for the [Department/Office] to access the PCD to inspect and copy the work-related data (e.g., for litigation purposes, public records retention and release obligations, internal investigations).
 - 2. Use of and data within a personally owned PCD may be discoverable in cases when there is reason to believe it is associated with work-related misconduct.
 - 3. Searches of a personally owned PCD by the [Department/Office] should be limited to those matters reasonably associated with the work-related business or work-related misconduct.
- (e) The device shall not be utilized to record or disclose any [department/office] business-related information, including photographs, video, or the recording or transmittal of any information or material obtained or made accessible as a result of employment or appointment with the [Department/Office], without the express authorization of the Chief of Police or the authorized designee.
- (f) If the PCD is carried on-duty, members will provide the [Department/Office] with the telephone number of the device.
- (g) All work-related documents, emails, photographs, recordings, and other public records created or received on a member's personally owned PCD should be transferred to the South Salt Lake Police Department and deleted from the member's PCD as soon as reasonably practicable but no later than the end of the member's shift.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personal Communication Devices

Except with prior express authorization from their supervisors, members are not obligated or required to carry, access, monitor, or respond to electronic communications using a personally owned PCD while off-duty. If a member is in an authorized status that allows for appropriate compensation consistent with policy or existing collective bargaining agreements, or if the member has prior express authorization from their supervisor, the member may engage in [department/office] business-related communications. Should members engage in such approved off-duty communications or work, members entitled to compensation shall promptly document the time worked and communicate the information to their supervisors to ensure appropriate compensation. Members who independently document off-duty [department/office]-related business activities in any manner shall promptly provide the [Department/Office] with a copy of such records to ensure accurate recordkeeping.

702.6 USE OF PCD

The following protocols shall apply to all PCDs that are carried while on-duty or used to conduct [department/office] business:

- (a) A PCD shall not be carried in a manner that allows it to be visible while in uniform, unless it is in an approved carrier.
- (b) All PCDs in the workplace shall be set to silent or vibrate mode.
- (c) A PCD may not be used to conduct personal business while on-duty except for brief personal communications (e.g., informing family of extended hours). Members shall endeavor to limit their use of PCDs to authorized break times unless an emergency exists.
- (d) Members may use a PCD to communicate with other personnel in situations where the use of radio communications is either impracticable or not feasible. PCDs should not be used as a substitute for, as a way to avoid, or in lieu of regular radio communications.
- (e) Members are prohibited from taking pictures, audio or video recordings, or making copies of any such picture or recording media unless it is directly related to official [department/office] business. Disclosure of any such information to any third party through any means requires express authorization of the Chief of Police or the authorized designee.
- (f) Members will not access social networking sites for any purpose that is not official [department/office] business. This restriction does not apply to a personally owned PCD used during authorized break times.
- (g) Using PCDs to harass, threaten, coerce, or otherwise engage in inappropriate conduct with any third party is prohibited. Any member having knowledge of such conduct shall promptly notify a supervisor.

702.7 SUPERVISOR RESPONSIBILITIES

The responsibilities of supervisors include but are not limited to:

- (a) Ensuring that members under their command are provided appropriate training on the use of PCDs consistent with this policy.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personal Communication Devices

- (b) Monitoring, to the extent practicable, PCD use in the workplace and taking prompt corrective action if a member is observed or reported to be improperly using a PCD.
 - 1. An investigation into improper conduct should be promptly initiated when circumstances warrant.
 - 2. Before conducting any administrative search of a member's personally owned device, supervisors should consult with the Chief of Police or the authorized designee.

702.8 USE WHILE DRIVING

The use of a PCD while driving can adversely affect safety, cause unnecessary distractions, and present a negative image to the public. Officers operating emergency vehicles should restrict the use of these devices to matters of an urgent nature and should, where practicable, stop the vehicle at an appropriate location to use the PCD.

Except in an emergency, members who are operating non-emergency vehicles shall not use a PCD while driving unless the device is specifically designed and configured to allow hands-free use (Utah Code 41-6a-1716). Hands-free use should be restricted to business-related calls or calls of an urgent nature.

702.9 OFFICIAL USE

Members are reminded that PCDs are not secure devices and conversations may be intercepted or overheard. Caution should be exercised while utilizing PCDs to ensure that sensitive information is not inadvertently transmitted. As soon as reasonably possible, members shall conduct sensitive or private communications on a land-based or other [department/office] communications network.

Vehicle Maintenance

703.1 PURPOSE AND SCOPE

Employees are responsible for assisting in maintaining Department vehicles so that they are properly equipped, properly maintained, properly refueled and present a clean appearance.

703.2 DEFECTIVE VEHICLES

When a Department vehicle becomes inoperative or in need of repair that affects the safety of the vehicle, that vehicle shall be removed from service for repair. Proper documentation shall be promptly completed by the employee who first becomes aware of the defective condition, describing the correction needed. The paperwork shall be promptly forwarded to vehicle maintenance for repair.

703.2.1 DAMAGE OR POOR PERFORMANCE

Vehicles that may have been damaged, or perform poorly shall be removed from service for inspections and repairs as soon as practicable.

703.2.2 SEVERE USE

Vehicles operated under severe-use conditions, which include operations for which the vehicle is not designed or that exceed the manufacturer's parameters, should be removed from service and subjected to a safety inspection as soon as practicable. Such conditions may include rough roadway or off-road driving, hard or extended braking, pursuits or prolonged high-speed operation.

703.2.3 REMOVAL OF WEAPONS

All firearms, weapons and control devices shall be removed from a vehicle and properly secured in the department armory prior to the vehicle being released for maintenance, service or repair.

703.3 VEHICLE EQUIPMENT

Certain items shall be maintained in all Department vehicles for emergency purposes and to perform routine duties.

703.3.1 PATROL VEHICLES

Officers shall inspect the patrol vehicle at the beginning of the shift and ensure that the minimum equipment, as listed below, is present in the vehicle:

- 20 Emergency road flares
- 2 Sticks yellow crayon or chalk
- 1 Roll Crime Scene Barricade Tape
- 1 First aid kit, CPR mask
- 1 Blanket
- 1 Blood-borne pathogen kit, including protective gloves

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Maintenance

- 1 Sharps container
- 1 Hazardous waste disposal bag
- 1 Traffic Safety Vest
- 1 Hazardous Materials Emergency Response Handbook
- 1 Evidence collection kit
- 1 Camera

703.3.2 UNMARKED VEHICLES

An employee driving unmarked Department vehicles shall ensure that the minimum equipment, as listed below, is present in the vehicle:

- 20 Emergency road flares
- 1 Roll Crime Scene Barricade Tape
- 1 First aid kit, CPR mask
- 1 Blanket
- 1 Blood-borne pathogen kit, including protective gloves
- 1 Sharps container
- 1 Hazardous waste disposal bag
- 1 Traffic Safety Vest
- 1 Hazardous Materials Emergency Response Handbook
- 1 Evidence collection kit
- 1 Camera

703.4 VEHICLE REFUELING

- (a) Absent emergency conditions or supervisor approval, officers driving patrol vehicles shall not place a vehicle in service that has less than one-quarter tank of fuel. Vehicles shall only be refueled at the authorized location.
- (b) All South Salt Lake vehicles have an assigned gas card unique to the vehicle. Do not use a gas card from another vehicle. If the card is not in the vehicle or lost, it needs to be reported up the chain of command and to the Fleet Manager so that it can be replaced. A supervisor's gas card may be used until the proper card is replaced.
- (c) Damaged gas cards or gas cards that are unable to be processed at the pump, need to be reported up the chain of command and the Fleet Manager so the card can be replaced.
- (d) Always keep the gas card in the vehicle and in a safe place out of the public's view. Never keep a gas card in your wallet or purse, the gas card is City property and must remain in the vehicle assigned.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Maintenance

- (e) Gas cards are only authorized to purchase fuel for the assigned vehicle. Do not purchase car washes on the gas card.
- (f) Any unauthorized purchase could result in discipline, up to termination for misuse of the gas card.

703.4.1 INSTRUCTION FOR PROPER USE OF GAS CARD

- (a) Assigned PIN numbers are the employee's personal responsibility.
- (b) Never share your PIN number with anyone.
- (c) Use only fuel stations that accept GasCard and FuelMan Cards.
- (d) Swipe the vehicle's gas card at the pump before fueling.
- (e) An authorized fuel station will require two things: 1) the driver's PIN and 1) the odometer reading. The odometer reading must be entered accurately (no tenths)
- (f) If you forget your PIN number, do not guess. Three wrong PIN attempts will lock the gas card and it cannot be used. If this occurs, report through your chain of command and to the Fleet Manager. It can take 3-7 days to obtain a replacement.
- (g) A supervisor's card must be used until the proper card is reinstated.

703.5 WASHING OF VEHICLES

- (a) All units shall be kept clean at all times, and weather conditions permitting, shall be washed as necessary to enhance their appearance.
- (b) Only one marked unit should be at the car wash at a time unless otherwise approved by a supervisor.
- (c) Employees using a vehicle shall remove any trash or debris at the end of their shift. Confidential material should be placed in a designated receptacle provided for the shredding of this matter.
- (d) Smoking and chewing tobacco use is unauthorized in all City owned vehicles.
- (e) City owned vehicles, motorcycle and/or bikes will be cleaned before use at any community event.

703.6 CIVILIAN NON-SWORN EMPLOYEE USE

Non-sworn employees of the Police Department are not authorized to drive a marked vehicle. Civilian non-sworn employees assigned a vehicle or access to the use of a department owned vehicle must adhere to all applicable policies and laws.

Vehicle Use

704.1 PURPOSE AND SCOPE

The purpose of this policy is to establish a system of accountability to ensure [department/office] vehicles are used appropriately. This policy provides guidelines for on- and off-duty use of [department/office] vehicles and shall not be construed to create or imply any contractual obligation by the City of South Salt Lake to provide assigned take-home vehicles.

Additional guidelines for member responsibilities when transporting persons in custody may be found in the Transporting Persons in Custody Policy.

704.2 POLICY

The South Salt Lake Police Department provides vehicles for [department/office]-related business use and may assign patrol and unmarked vehicles based on a determination of operational efficiency, economic impact to the [Department/Office], requirements for tactical deployments, and other considerations.

704.2.1 DISCUSSION

The success of the "Car per Officer Program" requires the cooperation of every police officer. The main purpose of this program is to ensure the quickest possible response time to South Salt Lake in case of an emergency.

In addition, this policy establishes department-owned vehicle use off-duty. The restrictions are an effort to reduce the wear and tear the vehicle, and reduce City fuel expenses. The vehicles are not intended for use by officers as a primary means of off-duty transportation.

For the purpose of this policy section, the term "Officer" refers to any police department employee who is issued a department-owned vehicle.

704.2.2 VEHICLE PER OFFICER AND TAKE HOME PROGRAM

A police vehicle may be assigned to each officer in the department upon successful completion of the FTO Program. The police vehicle is assigned for use by the officer while on duty and for employment-related activities, subject to the following rules:

(a) Vehicle care and maintenance:

1. The vehicle exterior shall be washed regularly and the interior of the vehicle kept clean and neat at all times. Periodic inspections will be conducted by supervisors.
2. No alterations or changes will be made to the vehicle without prior approval of the officer's division commander.
 - (a) Window decals, ornaments hanging from the windshield mirror, bumper stickers or other signs, pictures or ornaments visible to the public are prohibited unless approved by the Chief of Police.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Use

3. The vehicle will be serviced at the city shops, at an interval directed by the Fleet Services Department.
 4. Officers will not transport pets or animals of any kind, or any building materials, in their assigned vehicles, nor will they carry heavy or excessive loads or have objects protruding from the trunk or window(s).
 - (a) Police Service Animals or animals being transported by the Animal Services Officer are exempt from section 4 above.
 5. The vehicle must be locked at all times when unattended and parked off the street, if possible, when not in use by the officer.
 - (a) The vehicle must be parked off the street when at the officer's residence.
 6. Department vehicles should not be left idling or unlocked and unattended where there is no legitimate reason to do so.
 7. Department equipment such as computers, weapons, badges, police identification, or clothing with police markings affixed will not be left in the vehicle when the officer is off duty, unless the vehicle is secured in a locked garage.
 8. When on vacation or left unattended for more than five days the vehicle must be left at the police department or secured in a locked garage.
 9. Each vehicle shall be equipped with all necessary paperwork and equipment.
 10. The use of tobacco is strictly prohibited in all city-owned vehicles. Officers will not use snuff or chewing tobacco, cigarettes, cigars, e-cigarettes and/or vape pens in police vehicles.
 - (a) The cost of necessary repairs to or refurbishment of any vehicle in which use of tobacco occurred will be the responsibility of the employee to which the vehicle was assigned.
- (b) Use of vehicle off-duty:
- (a) Officers will only use their department-owned vehicle to travel to and from work, to court and approved department training, and under the following circumstances:
 - (a) Incidental use during the officer's commute to and from work.
 - (b) For approved law enforcement related outside employment.
 - (c) While in "on-call" status.
 - (d) To travel to and from a gym, or fitness facility.
 - (e) While attending a department or city function.
 - (b) Officers who receive "on-call" pay for specific time periods are considered "on call" only for those time periods.
 - (c) "On-call" Officers may use their department-owned vehicle while in on-call status under the following circumstances:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Use

- (a) Personal use of the department-owned vehicle is allowed only when the officer resides within the forty-mile (40) limit or approved distance by the Chief of Police.
- (c) No person, except the officer assigned or police personnel, may drive the vehicle at any time, except in an emergency situation.
- (d) Abuse of the vehicle, violations of this policy or other related policies, may result in suspension or termination of the use of the vehicle in addition to other applicable sanctions or disciplinary action.
- (e) If an off-duty officer witnesses an egregious violation of the law, the officer should take enforcement action.
 - 1. The officer should take into consideration the nature of the offense, the officer's present abilities, and the presence of civilian passengers.
 - 2. Immediate notification should be made to dispatch to facilitate the recording of the time spent and action taken.
- (f) If the officer has passengers in the vehicle, the officer will not participate in any vehicle pursuits.
 - 1. If an emergency does arise, the passengers should be dropped off at a safe location before the officer becomes involved in a hazardous situation.
- (g) Officers shall carry proper identification, department authorized sidearm, handcuffs, portable radio and flashlight, while operating any department-owned vehicle.
- (h) When off-duty, officers may dress appropriately for their activities. When in contact with the public, attire should be suitable to represent the department.
- (i) Under no circumstances will department-owned vehicles be operated by any employee of the city who has a measurable amount of alcohol in their system.
- (j) The use of vehicle off-duty for approved law enforcement related outside employment is authorized.
- (k) The use of vehicle off-duty for non-law enforcement related outside employment is not authorized.

704.2.3 UNDERCOVER VEHICLES

Unassigned, unmarked units, shall not be used without first obtaining approval from the respective unit supervisor.

704.2.4 INSPECTIONS

The interior of any vehicle that has been used to transport any person other than an employee should be inspected prior to placing another person in the vehicle and again after the person is removed. This is to ensure that unauthorized items have not been left in the vehicle.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Vehicle Use

704.3 ACCIDENT DAMAGE, ABUSE AND MISUSE

- (a) Any time a vehicle is involved in a traffic collision, with another vehicle, an outside agency of authority will be requested to investigate the cause and responsibility. The supervisor of the employee involved in the collision shall complete the City-provided Vehicle Accident Form. This form will be forwarded to the appropriate division commander when completed. (Refer to Policy 502.4.1)
- (b) Any damage to a vehicle, not caused by a traffic collision, shall be immediately reported within the shift in which the damage was discovered, documented in memorandum format and forwarded to the shift sergeant.
- (c) An administrative investigation will be conducted to determine any vehicle abuse or misuse. If it is determined that misuse or abuse was a result of negligent conduct or operation, appropriate disciplinary action may result.

High Visibility Reflective Vests

705.1 PURPOSE AND SCOPE

- (a) This policy recognizes the inherent danger posed by vehicle traffic and the unavoidable exposure of police department employees to that danger while performing duties in or near traffic.
- (b) It shall be the policy of this department that any police department employee engaged in an activity that causes significant exposure to vehicle traffic shall wear a reflective traffic vest or other high visibility safety apparel issued or approved by the police department. Safety vests will be issued, other apparel to include jackets must be approved by the appropriate chain-of-command.
- (c) Activities intended by this policy include, but are not limited to, accident investigations, lane/road blockages, traffic control, stranded motorists and removing objects from the roadway.
- (d) For the purpose of this policy, enforcement functions such as, traffic stops, D.U.I. enforcement are exempt from this policy unless specifically directed by a sergeant or above.
- (e) Because not every circumstance can be listed where a reflective vest could be used to enhance the safety of officers, it is acceptable for sergeants and above to direct an employee to wear the vest at any time.

Uniform Requirements and Components

706.1 CLASS "A" OR DRESS UNIFORM (SWORN PERSONNEL)

- (a) Class "A" or Dress Uniform specifications:
- (b) The Class "A" or Dress uniform shall consist of:
 - 1. The regulation badge.
 - 2. The regulation hat and hat badge. Note: The dress hat will be mandatory at all funeral services
 - 3. Long sleeved navy shirt; (Refer to uniform profile at Skaggs Public Safety Uniforms & Equipment)
 - 4. Navy neck tie.
 - 5. Navy trousers; (Refer to uniform profile at Skaggs Public Safety Uniforms & Equipment)
 - 6. Metal nameplate; silver for officers and Sergeants; gold for Lieutenants and above.
 - 7. Service stars: optional, with one star representing five years of service.
 - 8. Black leather basket weave inner belt.
 - 9. Black leather basket weave duty belt with:
 - (a) Approved duty holster.
 - (b) Magazine pouch.
 - (c) Handcuff case.
 - 10. Black Bates Oxford high-gloss shoes.
 - 11. Female officers may wear small stud style earrings.

706.1.1 DRESS HAT

Dress Hat Specifications:

- (a) Bancroft 72pd Convertible (Navy blue) "" Silver metal braid for officers and Sergeants, gold metal braid for Lieutenants and above.
- (b) Keystone KUC R-13 (Navy blue) - Silver metal braid for officers and Sergeants, gold metal braid for Lieutenants and above.
- (c) The dress hat is worn only by sworn personnel. Non-sworn personnel are not authorized to wear the dress hat.

706.1.2 CLASS "B" UNIFORM

- (a) "Traditional" and "Utility" uniforms include:
 - 1. Leather or nylon duty belt.
 - 2. Metal badge and nameplate.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Uniform Requirements and Components

3. Specifications: (Refer to uniform profile at Skaggs Public Safety Uniforms & Equipment)
- (b) "Utility Embroidered" uniforms include:
 1. Nylon duty belt.
 2. Embroidered badge and name strip.
 3. Specifications: (Refer to uniform profile at Skaggs Public Safety Uniforms & Equipment)
 4. Embroidery will be as follows:
 - (a) Department "POLICE" badge embroidered over the left chest area of the shirt
 - (b) Officer's first initial and last name (Capitol and lower case, e.g. T. Jones) embroidered over the right chest area of the shirt.
 - (c) All lettering is to be "embroidery silver" in color.
 5. The uniform shirt will not display any medal pins or insignias.
 6. The "utility embroidered" uniform is not authorized for the rank of Lieutenant or above.
- (c) Uniform Shorts:
 - (a) Department-authorized shorts may be worn by sworn and non-sworn personnel as part of the daily uniform.
 - (b) The shorts are tailored from the regular duty pant, and are to be cut to just above the knee.
 - (c) Police Department personnel will wear: (Refer to uniform profile at Skaggs Public Safety Uniforms & Equipment)

706.1.3 "SOFT" UNIFORMS/C UNIFORM

- (a) Soft uniforms may be worn as an alternative to the Class "B" Uniform for detectives, community resource officers, front desk officer, school resource officer, youth service officer, and officers attending training.
- (b) Specifications: (Refer to uniform profile at Skaggs Public Safety Uniforms & Equipment)
- (c) All soft uniform shirts will be embroidered as follows:
 1. Department "POLICE" badge embroidered over the left chest area of the shirt.
 2. Officer's first initial and last name (Capitol i.e. T. JONES) embroidered over the right chest area of the shirt and title.
 3. "POLICE" (all capitol) embroidered on both sleeves, 1/2" above the cuff or shoulder patch.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Uniform Requirements and Components

4. All lettering is to be "embroidery silver" in color on officer's and sergeant's black shirts and "embroidery gold" in color for the rank of lieutenant and above on black shirts.
- 5.
- (d) Officers will carry the following equipment with the soft uniform:
 1. Department badge and identification card.
 2. Visible weapon with chambered round and magazine containing ammunition.
 3. One spare magazine loaded with ammunition.
 4. Handcuffs and keys.
 5. Body Worn Camera

706.1.4 K-9 UNIFORMS

- (a) Officer's assigned to K9 duties shall wear: (Refer to uniform profile at Skaggs Public Safety Uniforms & Equipment), with a nylon duty belt and accessories, cloth badge, embroidered name, and embroidered markings.

706.1.5 BIKE PATROL UNIFORMS

- (a) Officer's assigned to Bike Patrol unit will wear the specified uniform while working bike patrol or any special function involving the unit. The uniform will consist of the following:
 1. Refer to uniform profile at Skaggs Public Safety Uniforms & Equipment for uniform requirements.
 2. Nylon or leather duty belt and gear may be worn.

706.1.6 MOTOR UNIFORMS

- (a) Class "A" or Dress uniform:
 1. Regular duty breeches: (See below)
 2. Navy short sleeve shirt with "P" buttons: (Refer to uniform profile at Skaggs Public Safety Uniforms & Equipment).
 3. A Royal blue ascot.
 4. A lanyard, nameplate, badge, service stars and motor wings.
- (b) Winter Service:
 1. When weather conditions indicate, officer's may either wear the standard class "B" (patrol) uniform, or the cold weather gear approved by Police Administration.
- (c) Class "B" uniform:
 1. Regular duty breeches: (See below)

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Uniform Requirements and Components

2. Navy short sleeve shirt or long sleeve shirt: (Refer to uniform profile at Skaggs Public Safety Uniforms & Equipment).
 3. Badge.
 4. Silver nameplate.
 5. Service stars.
 6. Motor wings.
 7. Sergeants will also wear silver accessories.
- (d) Motor Breeches:
1. Refer to uniform profile at Skaggs Public Safety Uniforms & Equipment.
- (e) Helmet will be of white housing and black trim.
- (f) Coat: (Refer to uniform profile at Skaggs Public Safety Uniforms & Equipment).
- (g) Boots will be All American Boot Company brand, black all leather motor boot with P276 lug sole, cushion insole, lace-up front, side buckle at calf.
1. Standard Stocked Boot Part Number: ALL AA-905P276.
 2. Custom Made Boot Part Number: ALL AA-905L CUSTOM SIZE.

706.1.7 PLAIN CLOTHES ATTIRE FOR WORK, COURT, AND TRAINING

- (a) Male Officer's:
1. Business suit with tie.
 2. Slacks, dress shirt, tie and sport coat.
 3. Collared shirt with department logo, name and title.
 4. These items of clothing shall avoid extremes in material, style and color.
- (b) Female Officer's:
1. (a) Dress.
 - (b) Skirt or business slacks.
 - (c) Blazer.
 - (d) Blouses.
 - (e) Collared shirt with department logo, name and title
 - (f) These items of clothing shall avoid extremes in material, style and color.
- (c) The following items are not permitted:
- (a) Sweat suits, sweat pants, or sweat shirts (except Navy PD sweatshirt).
 - (b) Shorts.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Uniform Requirements and Components

- (c) T-shirts or any shirt without a collar.
- (d) Tennis shoes (other than black in color), sandals, or similar footwear.
- (d) Required Equipment while on-duty in plain-clothes attire:
 - (a) Department badge and identification card.
 - (b) Weapon with a chambered round and a magazine containing ammunition.
 - (c) One spare loaded ammunition magazine.
 - (d) Handcuffs and keys.
 - (e) Body Worn Camera
- (e) Exceptions:
 - (a) Officers assigned to "undercover" duty wherein it is necessary to conceal their identity as officers, may be excused by their Division Commander from the provisions of all or part of this policy.
 - (b) Officers assigned to light duty, as a result of injury.
- (f) Courtroom Attire:
 - (a) Male Officers or Professional Support Staff:
 - (a) Business suit with tie.
 - (b) Slacks, dress shirt, tie and sport coat.
 - (c) Department uniform Class A, B or C
 - (d) No jeans or t-shirt.
 - (b) Female Officers Professional Support Staff:
 - (a) Dress or business slacks.
 - (b) Skirt.
 - (c) Blazer.
 - (d) Blouses.
 - (e) Stud style or small hoop earring.
 - (f) Department uniform Class A, B or C
 - (g) No jeans or t-shirts.
- (g) Attire for Training, Conference, or Seminars:
 - 1. Department Training: Officers attending department training, may wear:
 - (a) Department uniform Class A, B, or C
 - (b) Courtroom Attire
 - (c) Clothing as required for the specific type of training, i.e. work out clothing for PT and Arrest Control.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Uniform Requirements and Components

- (d) Jeans and t-shirt are not acceptable to be worn at training, conference, or seminars.

706.1.8 PROFESSIONAL SUPPORT PERSONNEL UNIFORMS

- (a) The year-round uniform for Professional Support Personnel will consist of:
 - 1. Pants or Skirts neatly pressed and clean. Jeans maybe worn on Fridays.
 - 2. Shirts - Polo or golf style long or short sleeved, with name embroidered and PD logo.
 - 3. Cardigan sweater, jacket or sweatshirtwith current department logo embroidered.
 - 4. Purple logo shirts should be worn in October for Domestic Violence Awareness month, but may be worn year round.
 - 5. Navy Police Department Hoodie/Sweatshirt
 - 6. Jewelry worn should be professional style
 - 7. Items of clothing shall avoid extremes in material, style and color.
 - 8. Specifications:
 - (a) Refer to uniform profile at Skaggs Public Safety Uniforms & Equipment.

706.1.9 CROSSING GUARD UNIFORMS

- (a) All uniforms for Crossing Guards will be supplied by the Police Department. All requests for uniforms and accessories will be forwarded to the unit supervisor.

706.1.10 UNIFORM ACCESSORIES

- (a) The following uniform accessories are authorized for wear:
 - 1. Turtleneck:
 - (a) Black in color and in good repair.
 - (b) It may have the department initials "SSLPD" embroidered on the left side of the neck.
 - (c) The letters shall be white in color and inch in height.
 - (d) The turtleneck may only be worn with a long sleeve shirt or the sweater.
 - 2. Undershirt: White or black in color.
 - 3. Sweater V-Neck:
 - (a) LAPD blue 2x2 ribbed knit commando type, turn-back sleeves, reinforced patches on shoulders and sleeves.
 - (b) Blue w/ epaulets and badge/name holders.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Uniform Requirements and Components

- (c) The V-Neck Sweater will be worn over the uniform shirt, with the regulation tie.
- 4. Sweater Crew Neck:
 - (a) Same as the V-neck sweater specifications.
 - (b) The crew- neck sweater may be worn over the uniform shirt. A tie is not required.
 - (c) The uniform shirt need not be worn if the turtleneck is worn with this sweater.
- 5. Jackets:
 - (a) Unless specified below, the duty jacket will be police coats designed for police wear.
 - (b) It will be navy blue or black.
 - (c) It may have epaulets.
 - (d) If it has buttons they will be black or silver for patrol officers and Sergeants, and black or gold for Lieutenants and above.
 - (e) Outerwear will have the required patches and insignia as described in this policy.
 - (f) The cloth badge patch or metal badge may be worn on outerwear.
- g. Shoulder patches and name are required.
- 6. Tie: Navy blue clip-on or Velcro type.
- 7. Name tag: Silver for officers and Sergeants, gold for Lieutenants and above, both with black writing.
- 8. Body Armor: Level II or greater as approved by the Chief of Police or designee.
- 9. Rain Jacket: The rain jacket may be yellow, black or blue in color. It will also have "POLICE" on the back.
- 10. Jump Suit (coveralls):
 - (a) Black or LAPD Blue.
 - (b) It shall include the department badge (patch), embroidered name, and "POLICE" either embroidered or as a patch on the back.
 - (c) It shall also include the arm patch and appropriate rank insignia.
- 11. Nylon Gear: All will be black, of a high quality, and in good working condition. It may not be frayed, tattered or faded.
- 12. Shoes / Boots:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Uniform Requirements and Components

- (a) Uniform shoes will be all black in color.
 - (b) They can either be boots, dress type, or athletic type shoes.
 - (c) They will be primarily leather or synthetic leather in construction.
 - (d) Athletic shoes may be worn with all uniforms except the class "A" Uniform.
- 13. Socks:
 - (a) Will be black in color.
 - (b) White athletic socks will be worn with shorts. The athletic socks should cover the ankle and rest no higher than the bottom of the calf.
- 14. Riot Helmet:
 - (a) Shall be a hard-shelled helmet designed to protect the officer from blunt trauma and/or flying objects.
 - (b) It shall have a face shield and be black in color.
- 15. Ball Cap:
 - (a) The regulation ball cap will be navy blue for Patrol, black for K9 and Crime Scene.
 - (b) The cap shall be embroidered with the "South Salt Lake Police Department" logo.
 - (c) The Motor Unit can wear the approved Motors hat with their working uniform.
 - (d) The Police Administration must approve brand name and style.
- 16. Suspenders:
 - (a) Black Nylon Suspenders are authorized to be worn with the Class B utility uniform and nylon gun belt.
 - (b) Restrictions: The suspenders cannot be worn with the Class A uniform or Class B traditional uniform.
- (b) Restrictions / Exceptions:
 - (a) White gloves will not be worn unless specifically directed for special assignments.
 - (b) The epaulets may have Velcro fasteners or buttons. Epaulet buttons, if worn, will be gold for Lieutenants and above, silver for officers and Sergeants.
 - (c) The department badge and name-tag will be worn on the front of the sweater if it is worn as the outer garment. Badge and name-tag reinforcement patches will be sewn on the inside of the sweater.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Uniform Requirements and Components

- (d) Department patches will be worn on the sweater sleeves with the top edge against the shoulder seam of the sweater.
- (e) Rank insignia will be worn by ranking officers on the shoulder epaulets of the sweater insignia bars and clusters will be centered and 1" from the shoulder seam.
- (f) The sweater will be worn tucked in the trousers when the officer is wearing a duty uniform belt and equipment.

706.1.11 REQUIRED EQUIPMENT - OFF DUTY PERSONNEL

- (a) In addition to the officer's civilian clothing, the officer shall wear the authorized firearm and holster whenever in public places or when traveling on public streets and highways within the State of Utah.
- (b) RESTRICTIONS:
 - 1. Wearing a firearm in a bar or lounge, or public gathering place with the intent to consume alcohol is prohibited.
 - 2. When in civilian clothing, the weapon or holster shall not be exposed to public view except when necessary.

706.1.12 RANK, DEPARTMENT & UNIT INSIGNIA

- (a) All officers of the rank of Sergeant or above shall wear the insignia of their rank as provided in this section.
 - 1. Sergeant:
 - (a) The silver chevron pin shall be worn on each side of the shirt collar in a vertical position - single point up, centered between the top and bottom edge of the collar. (On the bike patrol shirt, Class A shirt, and leather coats only). The silver chevron pin maybe worn on the long or short sleeve navy Class B shirt with the pink Breast Cancer Awareness patch or the purple Domestic Violence Awareness patch.
 - (b) The regulation three-bar cloth chevron shall be worn on all jackets (except leather) and Class B shirts. The chevron shall be worn on each sleeve with the uppermost portion on the chevron one half inch below the lowermost portion of the shoulder patch.
 - 2. Lieutenant:
 - (a) The gold single-bar gilt pin will be worn on both sides of the shirt collar.
- (b) Shoulder emblem's:
 - (a) All uniformed personnel, with the exception of the Crossing Guards, shall have the official departmental shoulder emblem affixed to each shoulder of the uniform.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Uniform Requirements and Components

- (b) The patch shall be attached with the top of the patch one half inch below the sleeve head seam of all shirts and blouses and three quarters of an inch on all jackets. It shall be affixed in such a manner that a line bisecting the center of the patch shall be perpendicular to the ground when the garment is worn. The patch shall be sewn on the garment with colorfast thread and shall be machine stitched with black thread.
- (c) Service designation:
 - (a) One service star may be worn after completion of each five years of continuous service as a full time officer.
 - (b) The star(s) will be a part of the name-tag or placed right above the name-tag.

Cash Handling, Security and Management

707.1 PURPOSE AND SCOPE

This policy provides guidelines to ensure department members handle cash appropriately in the performance of their duties.

This policy does not address cash-handling issues specific to the Property and Evidence and Informants policies.

707.2 POLICY

It is the policy of the South Salt Lake Police Department to properly handle and document cash transactions and to maintain accurate records of cash transactions in order to protect the integrity of department operations and ensure the public trust.

707.3 PETTY CASH FUNDS

The Chief of Police shall designate a person as the fund manager responsible for maintaining and managing the petty cash fund.

Each petty cash fund requires the creation and maintenance of an accurate and current transaction ledger and the filing of invoices, receipts, cash transfer forms and expense reports by the fund manager.

707.4 PETTY CASH TRANSACTIONS

The fund manager shall document all transactions on the ledger and any other appropriate forms. Each person participating in the transaction shall sign or otherwise validate the ledger, attesting to the accuracy of the entry. Transactions should include the filing of an appropriate receipt, invoice or cash transfer form. Transactions that are not documented by a receipt, invoice or cash transfer form require an expense report.

707.5 PETTY CASH AUDITS

The fund manager shall perform an audit no less than once every six months. This audit requires that the fund manager and at least one command staff member, selected by the Chief of Police, review the transaction ledger and verify the accuracy of the accounting. The fund manager and the participating member shall sign or otherwise validate the ledger attesting to the accuracy of all documentation and fund accounting. A discrepancy in the audit requires documentation by those performing the audit and an immediate reporting of the discrepancy to the Chief of Police.

Transference of fund management to another member shall require a separate petty cash audit and involve a command staff member.

A separate audit of each petty cash fund should be completed on a random date, approximately once each year by the Chief of Police or the City.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Cash Handling, Security and Management

707.6 ROUTINE CASH HANDLING

Those who handle cash as part of their property or Street Crimes Unit supervisor duties shall discharge those duties in accordance with the Property and Evidence and Informants policies.

Members who routinely accept payment for department services shall discharge those duties in accordance with the procedures established for those tasks.

707.7 OTHER CASH HANDLING

Members of the Department who, within the course of their duties, are in possession of cash that is not their property or that is outside their defined cash-handling responsibilities shall, as soon as practicable, verify the amount, summon another member to verify their accounting, and process the cash for safekeeping or as evidence or found property, in accordance with the Property and Evidence Policy.

Cash in excess of \$1,000 requires immediate notification of a supervisor, special handling, verification and accounting by the supervisor. Each member involved in this process shall complete an appropriate report or record entry.

Chapter 8 - Support Services

Crime Analysis

800.1 PURPOSE AND SCOPE

The management analysis function is a set of systematic, analytical processes directed at providing timely and pertinent information relevant to crime patterns and correlations between trends. The intent of this process is to assist operational and administrative personnel with long term planning and deployment of resources in order to prevent or suppress criminal activities. As such and where practical, management analysis information may be used in the formation of department tactics, strategies and long-range plans.

For information to be most effective in guiding the department personnel and resources, it must be current. It is the responsibility of each individual supervisor of a unit to ensure that all information being gathered by their personnel is accurate.

800.2 DATA SOURCES

- (a) Management analysis is the responsibility of the department Crime Analyst. Through the direction and leadership of the Community Resource Sergeant, the Crime Analyst shall be responsible for the collection, collation, analysis, and dissemination of crime data.
- (b) Elements of Analysis:
 - 1. Analysis of crime and crime trends should be based upon current data collected as a result of departmental activities. This may include the use of crime and/or arrest reports, incident reports, calls for service logs, citations, field interview cards, investigative supplemental reports, etc. The data used in the management analysis function should be up-to-date, within a reasonable amount of time.
 - 2. Collation involves the sorting out and organizing of raw data into logical groupings for analysis purposes. It is accomplished by grouping data of like offenses together so that the analysis encompasses all available data for each crime being analyzed.
 - 3. Raw data can also be grouped together to show crime patterns according to geographic locations, times of days crimes occurred, and/or how long patterns have been occurring (days, weeks, months, etc.).
- (c) Reporting Crime Patterns or Trends:
 - 1. Whenever a pattern of criminal activity is identified, it will be reported via the chain of command to the Chief of Police.
- (d) Dissemination of Analyzed Crime Information:
 - 1. Management analysis information must be shared for it to be of any use in combating future occurrences of crime. Dissemination of analysis information

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Crime Analysis

is the responsibility of the data processing person(s), and should include the sharing of information, for use, with:

- (a) The Chief of Police.
 - (b) Division Command.
 - (c) Section Command.
 - (d) Unit Command.
 - (e) Department Planning Personnel.
 - (f) News Media
 - (g) Others as appropriate.
- (e) Target Offenses:
- (a) When a trend in the occurrence of a particular crime(s) is identified, the information should be communicated, as per this order. Additionally, the documented times and geographic distributions of such crimes.
 - (b) A graphic representation of the crime distribution for each crime may also be created by the crime analyst and disseminated per this order.
- (f) Public Dissemination:
- (a) When crime trends are identified that appear to be ongoing or long-range in scope, a general report of the trends should be prepared.
 - (b) The report should not contain specific information useful in any investigation, nor should it describe suspects, modus operandi or other information that would jeopardize department operations.
 - (c) The report will be forwarded to the Chief of Police via the chain of command.
 - (d) Upon the Chief's approval, the department's public information officer may disseminate the report to the public.
- (g) Analysis Feedback:
- (a) Feedback is needed from users of disseminated information regarding the validity, reliability and usefulness of the information presented. As such, input from end-users of analysis information that reflects any discrepancies should be forwarded. The input should be based upon any action taken by operational units as a result of any analysis data disseminated.
 - (b) The data processing unit, or representative, should meet with the division commanders on a regular basis to discuss current patterns and trends of criminal behavior.
- (h) Re-occurring Statistical Reporting:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Crime Analysis

- (a) On a monthly basis, the Crime Analyst will assist the division commanders and the Office of the Chief of Police in the formulation of their month end reporting needs
- (b) On a annual basis the Crime Analyst will compile a year-end statistical report for the Chief of Police.

800.3 CRIME ANALYSIS FACTORS

The following minimum criteria should be used in collecting data for crime analysis:

- Frequency by type of crime
- Geographic factors
- Temporal factors
- Victim and target descriptors
- Suspect descriptors
- Suspect vehicle descriptors
- Modus operandi factors
- Physical evidence information

800.4 CRIME ANALYSIS DISSEMINATION

- (a) The task of data analysis includes compilation of statistical information, verification and evaluation of the accuracy of information, identifying and analyzing methods of operation of individual criminals, providing crime pattern recognition, and identifying trends in crime occurrences. Factors included are:
 - 1. Frequency by type of crime.
 - 2. Geographical factors.
 - 3. Temporal factors.
 - 4. Chronological factors.
 - 5. Victim and target descriptors.
 - 6. Suspect descriptors.
 - 7. Suspect vehicle descriptors.
 - 8. Modus Operandi factors.
 - 9. Physical evidence information.
- (b) Data analysis efforts should also be directed at identifying similarities among different offenses, revealing commonalities and patterns in the characteristics of current crime problems, assisting in the screening and ordering of lists of suspects, and aiding in the

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Crime Analysis

assembling and classification of specific crimes that may involve an offender already in custody.

Property and Evidence

801.1 PURPOSE AND SCOPE

This policy provides for the proper collection, storage and security of evidence and other property. Additionally, this policy provides for the protection of the chain of evidence and those persons authorized to remove and/or destroy property.

801.2 DEFINITIONS

Definitions related to this policy include:

Cohabitant - A person who is 18 years old or older, who resides in the same residence as the owner cohabitant, and is any of the following (Utah Code 53-5a-501):

- Living as if a spouse of the owner cohabitant
- Related by blood or marriage to the owner cohabitant
- Has one or more children in common with the owner cohabitant
- Has an interest in the safety and well-being of the owner cohabitant

Evidence - Includes items taken or recovered in the course of an investigation that may be used in the prosecution of a case. This includes photographs and latent fingerprints.

Found Property - Includes property found by an employee or citizen that has no apparent evidentiary value, and where the owner cannot be readily identified or contacted.

Owner cohabitant - A cohabitant who is 18 years old or older and owns a firearm (Utah Code 53-5c-102).

Property - Includes all items of evidence, items taken for safekeeping, and found property.

Safekeeping - Includes the following types of property:

- Property obtained by the [Department/Office] for safekeeping such as a firearm
- Personal property of an arrestee not taken as evidence
- Property taken for safekeeping under authority of a law

801.3 PROPERTY HANDLING

Any employee who first comes into possession of any property shall retain such property in their possession until it is properly tagged and placed in the designated property locker or storage room along with a Property Form. Care shall be taken to maintain the chain of custody for all evidence.

Where ownership can be established as to found property with no apparent evidentiary value, such property may be released to the owner without the need for booking. The Property Form must be completed to document the release of property not booked and the owner shall sign the form acknowledging receipt of the item.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Property and Evidence

801.3.1 PROPERTY BOOKING PROCEDURE

All property must be booked prior to the employee going off-duty unless otherwise approved by a supervisor. Employees booking property should observe the following guidelines.

- (a) Complete the property screen in the RMS describing each item of property separately, listing all serial numbers, owner's name, finder's name and other identifying information or markings.
- (b) Mark each item of evidence with the booking employee's initials and the date booked using the appropriate method so as not to deface or damage the value of the property.
- (c) Complete an evidence/property tag and attach it to each package or envelope in which the property is stored.
- (d) Place the case number in the upper right hand corner of the bag.
- (e) The original Property Form shall be submitted with the case report. A copy shall be placed with the property in the temporary property locker or with the property if property is stored somewhere other than a property locker.
- (f) When the property is too large to be placed in a locker, the item may be retained by patrol evidence lockers. Submit the completed property record into a numbered locker indicating the location of the property.

801.3.2 SPECIAL SECURITY AND CONTROL MEASURES

Refer to subsections to properly process evidence items that need additional security and control measures; narcotics and dangerous drugs, explosives, exceptional handling of money and high value items and firearms.

801.3.3 NARCOTICS AND DANGEROUS DRUGS

All narcotics and dangerous drugs shall be booked separately completing the property report in RMS Paraphernalia as defined by Utah Code 58-37a-3 shall also be booked separately from the other drugs with a separate compelling the property report in RMS.

Nik testing of any narcotic or dangerous drug should be tested with a partner present and prepared to utilize a Naloxone Rescue Kit per instructions and training.

The officer seizing the narcotics and dangerous drugs shall place them in an evidence locker. All designated property or evidence forms will be completed in RMS. The remaining copy will be detached and submitted with the case report.

801.3.4 EXPLOSIVES

Officers who encounter a suspected explosive device shall promptly notify their immediate supervisor or the Watch Commander. The bomb squad will be called to handle explosive-related incidents and will be responsible for the handling, storage, sampling and disposal of all suspected explosives.

Explosives will not be retained in the police facility. Only fireworks that are considered stable and safe and road flares or similar signaling devices may be booked into property. All such items shall be stored in proper containers and in an area designated for the storage of flammable materials.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Property and Evidence

The property and evidence technician is responsible for transporting to the fire department, on a regular basis, any fireworks or signaling devices that are not retained as evidence.

801.3.5 EXCEPTIONAL HANDLING

Certain property items require a separate process. The following items shall be processed in the described manner:

- (a) Bodily fluids such as blood or semen stains shall be air dried prior to booking.
- (b) License plates found not to be stolen or connected with a known crime should be released directly to the property and evidence technician or placed in the designated container for return to the Utah Division of Motor Vehicles. No formal property booking process is required.
- (c) All bicycles and bicycle frames require a property report. Property tags will be securely attached to each bicycle or bicycle frame. The property may be released directly to the property and evidence technician or placed in the bicycle storage area until a property and evidence technician can log it in.
- (d) All cash shall be counted in the presence of a supervisor and the envelope initialed by the booking officer and the supervisor. The Watch Commander shall be contacted for cash in excess of \$1,000 for special handling procedures, which includes the watch commander signing off on the amount and notifying evidence of the submission via email.
- (e) If any amount of monies, is obtained in excess of \$10,000, the watch commander will notify the deputy chief.

City property, unless connected to a known criminal case, should be released directly to the appropriate City department. No formal booking is required. In cases where no responsible person can be located, the property should be booked for safekeeping in the normal manner.

801.3.6 FIREARMS SAFE HARBOR ACT

Officers shall accept a firearm for safekeeping from any cohabitant or owner cohabitant who requests it, and who believes that the owner cohabitant or another cohabitant with access to the firearm is an immediate threat to the cohabitant, the owner cohabitant, or any other individual (Utah Code 53-5a-502).

The officer receiving the firearm shall:

- (a) Record the owner cohabitant's name, address, and telephone number.
- (b) Record the firearm's serial number and the make and model of each firearm received.
- (c) Record the date that the firearm was accepted for safekeeping.
- (d) If the firearm was received from a cohabitant, require that the cohabitant sign a document attesting that the cohabitant resides in a home with the owner cohabitant.

An owner cohabitant committing the firearm shall not be asked or required to provide the name of, or any other information about, the cohabitant who poses the threat.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Property and Evidence

If a firearm received under the Act is determined to be illegal to possess or to own, the property and evidence technician shall confiscate and book the firearm according to current procedures, notify the person who requested that the firearm be taken for safekeeping of its confiscation, and dispose of the firearm in accordance with Utah Code 77-11a-403 (Utah Code 53-5a-503).

The property and evidence technician shall hold a firearm accepted pursuant to this policy for an initial period of 60 days, renewable for an additional 60 days upon request of the cohabitant or owner cohabitant. At the expiration of this time the firearm shall be returned to the owner cohabitant subject to the following (Utah Code 53-5a-502; Utah Code 53-5a-503):

- If, prior to the expiration of the 60-day period, the owner cohabitant requests return of the firearm in person, it shall be returned at the time of the request.
- If an owner other than the owner cohabitant requests return of the firearm, it may be returned to such owner after the expiration of the 60-day period if the owner requesting the firearm provides identification and signs a document attesting to having ownership in the firearm or pursuant to a court order. Have the owner fill out a witness statement and bring any supporting paper work to verify ownership.
- If an owner is subject to a jail release agreement or jail release order arising out of a class A misdemeanor or felony domestic violence offense for which the owner was arrested and jailed and for which a court has determined probable cause exists, the firearm may not be returned until 60 days after the expiration of the jail release agreement or jail release order.
- The firearm may not be returned to the owner cohabitant if the owner cohabitant is a restricted person under Utah Code 76-11-302 or Utah Code 76-11-303 or otherwise prohibited from possessing a firearm under state or federal law.

If more than one year has passed since the firearm was committed and the owner cohabitant cannot be located, the [Department/Office] should dispose of the firearm in accordance with Utah Code 77-11a-403 (Utah Code 53-5a-503).

The property and evidence technician shall destroy any record created exclusively to document the safekeeping of the firearm as soon as practicable but no later than five days after releasing the firearm to the owner, or otherwise disposing of the firearm under the Utah Firearms Safe Harbor Act (Utah Code 53-5a-502).

801.4 PACKAGING OF PROPERTY

Certain items require special consideration and shall be booked separately as follows:

- (a) Narcotics and dangerous drugs.
- (b) Firearms (ensure they are unloaded and booked separately from ammunition).
- (c) Property with more than one known owner.
- (d) Paraphernalia as described in Utah Code 58-37a-3.
- (e) Fireworks.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Property and Evidence

- (f) Contraband.

801.4.1 PACKAGING CONTAINER

Employees shall package all property, except narcotics and dangerous drugs, in a suitable container available for its size. Knife boxes should be used to package knives, and syringe tubes should be used to package syringes and needles.

A property tag shall be securely attached to the outside of all items or group of items packaged together.

801.4.2 PACKAGING NARCOTICS

The officer seizing narcotics and dangerous drugs shall retain such property in their possession until it is properly weighed, packaged, tagged and placed in an evidence locker. Prior to packaging, and if the quantity allows, a presumptive test should be made on all suspected narcotics. If conducted, the results of this test shall be included in the officer's report.

Narcotics and dangerous drugs shall be packaged in an envelope of appropriate size available in the report room. The booking officer shall initial the sealed envelope and the initials covered with cellophane tape. Narcotics and dangerous drugs shall not be packaged with other property.

A completed property tag shall be attached to the outside of the container. Evidence Technicians will record the evidence submission through the case management system.

801.5 RECORDING OF PROPERTY

The property and evidence technician receiving custody of evidence or property shall follow RMS procedure.

A property number shall be obtained for each item or group of items. This number shall be recorded on the property tag.

Any changes in the location of property held by the South Salt Lake Police Department shall be noted in RMS.

801.6 PROPERTY CONTROL

Each time the property and evidence technician receives property or releases property to another person, he/she shall enter this information into the RMS system. Officers desiring property for court shall contact the property and evidence technician at least one day prior to the court date.

801.6.1 RESPONSIBILITY OF OTHER PERSONNEL

Every time property is released or received, an appropriate entry into the case management system shall be completed to maintain the chain of possession. No property or evidence is to be released without first receiving written authorization from a supervisor or detective.

Request for analysis of items other than narcotics or drugs shall be submitted to the property and evidence technician via email. This request may be filled out any time after booking of the property or evidence.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Property and Evidence

801.6.2 TRANSFER OF EVIDENCE TO CRIME LABORATORY

The transporting employee will check the evidence out of property, indicating the date and time in the case management system.

All toxicology and crime lab analysis request are submitted through UCJIS by the evidence technicians, Evidence technicians submit all the evidence data into the case management system.

801.6.3 STATUS OF PROPERTY

Each person receiving property will make the appropriate entry to document the chain of evidence. Temporary release of property to officers for investigative purposes, or for court, shall be noted in the case management system. stating the date, time and to whom released.

The property and evidence technician shall obtain the signature of the person to whom property is released, and the reason for release. Any employee receiving property shall be responsible for such property until it is properly returned to property or properly released to another authorized person or entity.

The release and return of any property should be recorded in the case management system. indicating date, time and the person who it was released to or returned from.

801.6.4 RELEASE OF PROPERTY

The Investigations Division shall authorize the release of all property coming into the care and custody of the [Department/Office].

Release of property shall be made upon receipt of an authorized property release form, listing the name and address of the person to whom the property is to be released. The property release form shall be signed by the authorizing supervisor or investigator and must conform to the items listed on the property control card or must specify the specific items to be released. Release of all property shall be documented on the property control card.

Firearms or ammunition should only be released upon presentation of valid identification and authorized documents showing that the individual may legally possess the item.

All reasonable attempts shall be made to identify the rightful owner of found property and items held for safekeeping (Utah Code 77-11d-104). A property and evidence technician shall release such property when the owner presents proper identification, and an authorized property release form has been received. The signature of the person receiving the property and the final disposition of the property shall be recorded on the property control card.

Found property and property held for safekeeping shall be held for a minimum of 90 days. If the owner of any unclaimed property cannot be determined or notified, or if the owner has been notified and fails to appear and claim the property, the agency shall (Utah Code 77-11d-105):

- (a) Publish at least one notice (giving a general description of the property and the date of intended disposition) of the intent to dispose of the unclaimed property on the state Public Legal Notice website.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Property and Evidence

- (b) Post a similar notice in a public place designated for notice within the law enforcement agency.
- (c) Post a similar notice on the City public website of the South Salt Lake Police Department.

If no claim is made for the property, the property may be returned to the person who brought the property to the [Department/Office] or disposed of according to Utah Code 77-11d-105. The final disposition of the property shall be fully documented on the property control card.

801.6.5 DISPUTED CLAIMS TO PROPERTY

Occasionally more than one party may claim an interest in property being held by the [Department/Office], and the legal rights of the parties cannot be clearly established. Such property shall not be released until one party has obtained a valid court order or other undisputed right to the involved property.

All parties should be advised that their claims are civil and in extreme situations, legal counsel for the [Department/Office] may wish to file an interpleader to resolve the disputed claim.

801.6.6 CONTROL OF NARCOTICS AND DANGEROUS DRUGS

The Investigations Division will be responsible for the storage, control and destruction of all narcotics and dangerous drugs coming into the custody of the [Department/Office], including paraphernalia as described in Utah Code 58-37a-3.

801.7 DISPOSITION OF PROPERTY

1. Found Property

The investigating officer will attempt to determine and contact the owner(s) of found property at the time the property is recovered. The Property Officer will attempt to contact the owner(s) upon receipt and storage of the property.

- (a) When the owner has been identified, that person will be called on the telephone or notified via mail instructing them to contact the Property Officer to schedule an appointment to claim their property.
- (b) The owner will be given 90 days to establish ownership and claim the property.
- (c) If the property is not claimed, it will be offered to the finder (unless the finder is a City of South Salt Lake employee). The claimant will be given 90 days to claim the property. Exception: Unclaimed firearms will be disposed per state law. The Property Officer will notify the finder requesting them to schedule an appointment to obtain the property.
- (d) If the property is not claimed, the finder is legally entitled to the property.
- (e) All unclaimed property will be disposed of or auctioned.
- (f) Release to Finder
 - 1. The finder must present satisfactory evidence of identification and must sign to acknowledge receipt of the property to them.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Property and Evidence

2. The property report is removed from the property file and forwarded to Records for filing in the original case.

2. Safekeeping

Property that is being held for safekeeping shall be returned to the legal owner upon request or by legal mandate. Property (excluding firearms) not claimed within 3 months from the day of receipt shall be considered intentionally abandoned by the owner and will be disposed of as appropriate.

- (a) The Property Officer shall do the following upon receiving a firearm taken for safekeeping:
 - (a) Conduct a criminal history check on the owner or person from whom the weapon was taken.
 - (b) Conduct an NCIC check on the firearm to determine if it has been reported stolen. If stolen, first contact an investigator and notify them of the firearm's status. At the appropriate time, an attempt will be made to return the firearm to the rightful owner. If the owner cannot be found, the weapon will be disposed of per state law.
 - (c) Complete a firearm release request and forward to the investigating officer for approval to release.
 - (d) Upon return of the release form, the Property Officer will notify the owner by mail or telephone to schedule an appointment for release of the weapon.
 - (a) Release the weapon to the owner.
 - (b) The owner must present a photo ID and provide proof of ownership if requested.
 - (c) The owner must sign the release.
 - (d) The release is removed from the property file if there are no additional items of evidence connected with the case, and forwarded to Records for filing in the original case.
- (e) All other types of property held for safekeeping shall be returned to the owner as soon as possible.

Note: If the true owner is the person committing the crime for which the weapon was used as evidence, the department shall confiscate it and it shall revert to that agency for their use and/or disposal as the head of the department determines. Utah Code 76-10-525

- (b) Upon receiving property held for safekeeping, the handling case Officer shall do the following:
 - (a) Conduct an NCIC check on all serialized property to determine if it is stolen.
 - (b) Contact the owner by mail to schedule an appointment for the release of the property.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Property and Evidence

- (c) Property (except firearms) not claimed within 3 months from the day of receipt days is to be considered intentional abandonment by the owner and disposed of per statute.
- (d) Release to the owner:
 - The owner must present a photo ID and provide proof of ownership if requested. The owner must sign the property release. The property release is removed from the property file if there are no additional items of evidence connected with the case, and documented in the case management system.

3. Recovered Property

Property may be released by the Property Officer to the rightful owners prior to the conclusion of a trial under the authority of a court order, upon the written authorization of the representing prosecutor, or as otherwise provided by this manual.

- (a) Prior to release, a picture of the property and the owner will be taken by the investigating officer.
- (b) The owner must sign a Declaration of Ownership and agree not to destroy, sell, or give away the property until the conclusion of legal proceedings.
- (c) The person from whom the property was taken will have already received written notification of their right to claim the property.
 - (a) A copy of the notification will be attached to the property report. (ii) If a claim has been made, the magistrate will determine ownership.
- (d) The investigating officer must complete a property release form itemizing the property to be released and forward it to the Property Officer.
 - (a) The person must present a photo ID.
 - (b) The person must sign the property release form.
 - (c) All required information is submitted through the case management system.

4. Non-Essential Property/Evidence

- (a) With the concurrence of the prosecutor, property which is not essential to a prosecution or future prosecution shall be promptly released, whenever possible, to the owner as follows:
 - 1. Property (a photograph of which is sufficient for court presentation) shall be released, with the concurrence of the prosecuting District Attorney, to the rightful owner.
- (b) Whenever possible, property which the prosecutor considers to be non-essential to a prosecution shall be promptly released to the owner during the course of the investigation.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Property and Evidence

1. Property which has no market value or investigative value as determined by the prosecutor may be destroyed upon completion of the investigation; e.g., glass fragments, mutilated bullet not suitable for comparison purposes.
- (c) Property that has been held as evidence but not introduced during the trial shall be released to the owner upon receipt of a court disposition, provided the defendant has not filed an appeal within the prescribed time.
 1. In misdemeanor and felony cases, 90 days shall be allowed for an appeal after the sentence is imposed.
- (d) Property that is to be held as potential evidence shall be disposed of in accordance with the provisions of this manual as appropriate.
 1. (i) In all cases, the person who receives the property must present a photo ID.
 2. (ii) The property release must be signed by the person accepting the property.
 3. (iii) If all of the recorded property has been returned to the owner, and documented in the case management system.

5. Court Releases

- (a) When the Property Officer receives an evidence request form, or is contacted by the person needing evidence for court, the item(s) needed shall be pulled from its storage location and released
 - (a) In all cases, the person who receives the property must present a photo ID.
 - (b) The property release must be signed by the person accepting the property.
 - (c) If all of the recorded property has been returned to the owner, the property release is removed from the property file.

801.7.1 EXCEPTIONAL DISPOSITIONS

The following types of property shall be destroyed or disposed of in the manner, and at the time prescribed by law, unless a different disposition is ordered by a court of competent jurisdiction:

- Weapons declared by law to be nuisances
- Animals, birds, and related equipment that have been ordered forfeited by the court
- Counterfeiting equipment
- Gaming devices
- Obscene matter ordered to be destroyed by the court
- Altered vehicles or component parts
- Narcotics (Utah Code 58-37-2 et seq.)
- Unclaimed, stolen or embezzled property
- Destructive devices

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Property and Evidence

801.7.2 UNCLAIMED MONEY

If found or seized money is no longer required as evidence and remains unclaimed after nine days of being posted, as described in Release of Property, the [Department/Office] shall notify the person who turned the money over to the [Department/Office]. Any person employed by a law enforcement agency who finds or seizes money may not claim or receive the money (Utah Code 77-11d-105).

801.7.3 BIOLOGICAL EVIDENCE

The property and evidence technician shall ensure that no biological evidence held by this [department/office] is destroyed without adequate notification to the following persons, when applicable:

- (a) The defendant
- (b) The defendant's attorney
- (c) The appropriate prosecutor and Attorney General
- (d) Any sexual assault victim
- (e) The Investigation Division Commander

Biological evidence shall be retained for a minimum period established by law (Utah Code 77-11c-201; Utah Code 77-11c-301; Utah Code 77-11c-401; Utah Code 53-10-904; Utah Code 53-10-905) or the expiration of any sentence imposed related to the evidence, whichever time period is greater. Following the retention period, notifications should be made by certified mail and should inform the recipient that the evidence will be destroyed after a date specified in the notice, unless a motion seeking an order to retain the sample is filed and served on this [department/office] within 90 days of the date of the notification. A record of all certified mail receipts shall be retained in the appropriate file. Any objection to, or motion regarding, the destruction of the biological evidence should be retained in the appropriate file and a copy forwarded to the Investigation Division Commander.

Biological evidence related to a homicide shall be retained indefinitely and may only be destroyed with the written approval of the Chief of Police and the head of the applicable prosecutor's office.

Biological evidence from an unsolved sexual offense should not be disposed of prior to expiration of the statute of limitations. Even after expiration of the applicable statute of limitations, the Investigation Division Commander should be consulted and the sexual assault victim should be notified.

801.7.4 PROPERTY NO LONGER NEEDED AS EVIDENCE

When a prosecuting attorney notifies the [Department/Office] that evidence may be returned to the rightful owner, the property and evidence technician shall attempt to notify the rightful owner that the property is available for return. Prior to the release of the property, the owner shall provide (Utah Code 77-11a-301):

- (a) Documentation establishing ownership of the property.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Property and Evidence

- (b) Documentation that the owner may lawfully possess the property.

Before returning a seized firearm to an owner, the property and evidence technician shall confirm through the Bureau of Criminal Identification, that the owner is eligible to lawfully possess and receive a firearm (Utah Code 24-3-103).

When the property is returned, a receipt listing the detail of the property shall be signed by the owner and retained by the [Department/Office]. A copy of the receipt shall be provided to the owner (Utah Code 77-11a-301).

If the [Department/Office] is unable to locate the rightful owner or the rightful owner is unable to lawfully possess the property, the [Department/Office] may dispose of the property as provided by Utah Code 77-11a-402.

If a court orders extraction and return of personal digital data from a computer determined to be contraband, the [Department/Office] shall determine reasonable cost to provide the data, which shall be paid by the owner at the time the request is made (Utah Code 77-11a-301).

The [Department/Office] shall dispose of confiscated or unclaimed firearms as provided by Utah Code 77-11a-403.

801.7.5 SEXUAL ASSAULT KITS

Written notification shall be provided to a victim of the intent to destroy or dispose of a sexual assault kit evidence or other crime scene evidence from an unsolved sexual assault case within 60 days prior to the destruction or disposal (Utah Code 77-37-3).

801.8 INSPECTIONS OF THE EVIDENCE ROOM

- (a) On a monthly basis, the supervisor of the evidence custodian shall make an inspection of the evidence storage facilities and practices to ensure adherence to appropriate policies and procedures.
- (b) Unannounced inspections of evidence storage areas shall be conducted annually as directed by the Chief of Police.
- (c) An annual audit of evidence held by the [Department/Office] shall be conducted by a Division Commander (as appointed by the Chief of Police) not charged with custody of property.
- (d) Whenever a change is made in personnel who have access to the Evidence Room, an inventory of all evidence/property shall be made by an individual(s) not associated with the property room or its functions to ensure that records are correct and all evidence and property is accounted for.

801.9 ADMITTANCE TO EVIDENCE ROOM

Admittance to the Evidence Room should be restricted to the evidence custodian(s), the evidence supervisor, and others specifically designated by the Chief of Police. All other individuals entering the Evidence Room require escort and an Evidence Room access log entry shall be made indicating:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Property and Evidence

- (a) Date and time of entry and exit.
- (b) Name of individual(s) entering the Evidence Room.
- (c) Reason for entry.
- (d) Name of the escort.

801.10 DESTRUCTION, DONATION, DIVERSION AND AUCTIONING OF PROPERTY

The Destruction, Donation, Diversion and Auctioning of items from Evidence/Property will take place only after proper authorization and in accordance with State Law and the authorized South Salt Lake Police Evidence Room Procedures.

Records Section

802.1 PURPOSE AND SCOPE

This policy establishes the guidelines for the operational functions of the South Salt Lake Police Department Records Section. The policy addresses [department/office] file access and internal requests for case reports.

802.2 POLICY

It is the policy of the South Salt Lake Police Department to maintain [department/office] records securely, professionally, and efficiently.

802.3 FILE ACCESS AND SECURITY

The security of files in the Records Section must be a high priority and shall be maintained as mandated by state or federal law. All case reports including but not limited to initial, supplemental, follow-up, evidence, and any other reports related to a police [department/office] case, including field interview (FI) cards, criminal history records, and publicly accessible logs, shall be maintained in a secure area within the Records Section accessible only by authorized members of the Records Section. Access to case reports or files when Records Section staff is not available may be obtained through the Watch Commander.

The Records Section will also maintain a secure file for case reports deemed by the Chief of Police as sensitive or otherwise requiring extraordinary access restrictions.

802.3.1 ORIGINAL CASE REPORTS

Generally, original case reports shall not be removed from the Records Section. Should an original case report be needed for any reason, the requesting [department/office] member shall first obtain authorization from the Records Supervisor. All original case reports removed from the Records Section shall be recorded on a designated report check-out log, which shall be the only authorized manner by which an original case report may be removed from the Records Section.

All original case reports to be removed from the Records Section shall be photocopied and the photocopy retained in the file location of the original case report until the original is returned to the Records Section. The photocopied report shall be shredded upon return of the original report to the file.

802.4 CONFIDENTIALITY

Records Section staff has access to information that may be confidential or sensitive in nature. Records Section staff shall not access, view, or distribute, or allow anyone else to access, view, or distribute any record, file, or report, whether in hard copy or electronic file format, or any other confidential, protected, or sensitive information except in accordance with Records Maintenance and Release and Protected Information policies and the Records Section procedure manual.

802.5 RESPONSIBILITIES OF RECORDS TECHNICIANS

The responsibilities of the Records Technicians include but are not limited to:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Records Section

- (a) Maintaining a records management system for case reports.
 - 1. The records management system should include a process for numbering, identifying, tracking, and retrieving case reports.
- (b) Entering case report information into the records management system.
 - 1. Modification of case reports shall only be made when authorized by a supervisor.
- (c) Providing members of the department with access to case reports when needed for investigation or court proceedings.
- (d) Maintaining compliance with federal, state, and local regulations regarding reporting requirements of crime statistics. This included but is not limited to reporting:
 - 1. Crime reporting and use of force data to the Bureau of Criminal Identification (BCI) (Utah Code 53-10-205).
 - 2. Cold case reporting to the Criminal Investigations and Technical Services Division (Utah Code 53-10-115).
- (e) Maintaining compliance with federal, state, and local regulations regarding criminal history reports and auditing.
- (f) Identifying missing case reports and notifying the responsible member's supervisor.
- (g) Providing an annual report to BCI regarding firearm related information as required by Utah Code 76-10-526.
- (h) Receive, maintain, and remove voluntary restrictions on firearms purchase and possession in accordance with the Utah Code 53-5c-301. This includes required notifications to BCI (Utah Code 53-5c-301).

802.5.1 NCIC VALIDATION PROCEDURE

Each month the Utah Bureau of Criminal Identification (BCI) receives a file from National Crime Information Center (NCIC) records to be validated. BCI in turn distributes the records to be validated to the entering agency.

Per NCIC Manual specifications, validation obliges the entering agency to confirm that the record is complete, accurate, and still outstanding or active. Validation of NCIC records is the responsibility of the Records Division.

Validation is accomplished by reviewing the entry and current supporting documents (both electronic and/or hard copy), and by recent consultation with any appropriate complainant, victim, prosecutor,

court or other appropriate source or individual. Any information that has changed since the original entry, or is inaccurate, should be modified and updated.

Additionally, it is necessary to "pack" the record with as much information as possible, filling in all the fields for which information is available and adding comments in the miscellaneous field if there is additional information that cannot be included elsewhere on the record. Possible sources for new or updated information include, but are not limited to, Utah Criminal Justice Information System (UCJIS) files (driver license, motor vehicle, NCIC, criminal history records, etc.), initial

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Records Section

and supplemental narratives on the case report, initial call notes and documents attached to the original case file. In the event the entering agency is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the entry in the file. The agency must modify each record being validated to include updated information in the Name of Validator (VLN) Field. If a record has not been validated within a month from the request for validation, the NCIC System will generate a \$.F. Failure to Validate Notification to the entering agency on the Monday following the first Sunday of the month. The \$.F. notification serves as a warning for the agency to validate the record or the NCIC System will purge the record during the next purge cycle. If the record is not validated by the first Sunday of the following month, the NCIC System will purge the record and generate a \$.P. Purge Failure to Validate Notification. It is considered a serious compliance issue if an active record is purged by NCIC due to lack of validation.

Validation Certification and Response

The Records Division will validate each NCIC record on the validation listing provided each month.

Validation certification means that:

1. The records contained on the validation listing have been reviewed
2. The records which are no longer current have been removed from the NCIC database and all records remaining in the NCIC system are valid and active;
3. Records contain all available information. If any new information is available since entry/last validation, the record will be modified to reflect the additional information; and
4. The information contained in each of the records is accurate.

Once a record has been reviewed to ensure it is still current, complete and accurate, the individual who validated the record will put their initials and date of validation in the Name of Validator (VLN) Field of the Modify transaction of each record in UCJIS.

Documentation of Validation

For each NCIC file validated, the employee completing the validation shall fill out the validation form, indicating when the record was validated, who was contacted, any changes made to the entry and who

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Records Section

completed the validation. Additionally, the employee validating the record should print the validation

verification response from UCJIS and include it in the NCIC file. All validation documentation shall be

filed with the original entry paperwork, and the file shall be kept in the Records office, at all times, where it can be accessed 24 hours a day if needed for hit confirmation or any other reason.

REFERENCE INFORMATION

National Crime Information Center (NCIC) Operating Manual: <https://www.ojp.gov/ncjrs/virtual-library/abstracts/ncic-national-crime-information-center-operating-manual>

Utah Bureau of Criminal Identification (BCI): <https://bci.utah.gov/>

Utah Criminal Justice Information System (UCJIS) Help Desk: (801) 965-4446 or dpsic@utah.gov

802.5.2 RECORDS SUPERVISOR

The Chief of Police shall appoint and delegate certain responsibilities to a Records Supervisor. The Records Supervisor shall be directly responsible to the Administration Division Commander or the authorized designee.

The responsibilities of the Records Supervisor include but are not limited to:

- (a) Overseeing the efficient and effective operation of the Records Section.
- (b) Scheduling and maintaining Records Section time records.
- (c) Supervising, training, and evaluating Records Section staff.
- (d) Maintaining and updating a Records Section procedure manual.
- (e) Ensuring compliance with established policies and procedures.
- (f) Supervising the access, use, and release of protected information (see the Protected Information Policy).
- (g) Establishing security and access protocols for case reports designated as sensitive, where additional restrictions to access have been implemented. Sensitive reports may include but are not limited to:
 - 1. Homicides
 - 2. Cases involving [department/office] members or public officials
 - 3. Any case where restricted access is prudent

Records Management: Access Control, GRAMA request, Data Reporting, Arrest & Warrant Records

803.1 ACCESS CONTROL

Scope and Purpose

This policy applies to all personnel, including employees, contractors, and affiliates of the Law Enforcement Agency, who require access to Criminal Justice Information (CJI). The purpose of this policy is to establish controls to safeguard CJI by managing access based on job roles, physical and logical locations, network addresses, and temporal restrictions. The policy aims to ensure that access to CJI is authorized, authenticated, and appropriate to the user's role, while protecting the integrity and confidentiality of CJI.

(a) Access Control Mechanisms

- Access to CJI shall be controlled based on the following criteria:
 - (a) **Job assignment or function:** Access is granted according to the role of the user.
 - (b) **Physical location:** Access may be restricted to specific physical locations.
 - (c) **Logical location:** Access may be restricted based on logical groupings within the network.
 - (d) **Network addresses:** Access may vary based on whether the user is accessing from within the agency's network or from external locations.
 - (e) **Time-of-day and day-of-week/month restrictions:** Access may be limited to specific times.

(b) Guest Accounts

- All guest accounts for non-employees with access to the criminal justice network shall have an expiration date of one year or the work completion date, whichever occurs first.
- Guest accounts for private contractors must be sponsored by an authorized member of the administrative entity managing the resource.

(c) Inactive Accounts

- The Terminal Agency Coordinator (TAC) must disable all new accounts that have not been accessed within 30 days of creation.
- Accounts of individuals on extended leave (more than 30 days) should be disabled, except in cases where uninterrupted access is required. Such cases must be supported by a manager-approved request from the designated account administrator or assistant.

(d) Notification of Changes

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Records Management: Access Control, GRAMA request, Data Reporting, Arrest & Warrant Records

- The TAC must be informed if a user's information system usage or need-to-know changes, such as termination or transfer.
- For individuals assigned to another office for more than 90 days, the TAC will transfer the individual's account(s) to the new agency.
- (e) **Termination of Access**
 - The TAC will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency.
- (f) **Account Management Responsibilities**
 - The TAC has primary responsibility for managing user accounts, including:
 - Modifying user accounts due to name changes, accounting changes, permission changes, office transfers, etc.
 - Reviewing existing accounts for validity at least every 6 months.
 - Cooperating with authorized security teams during security incidents or audit reviews.
- (g) **System Use Notification**
 - An approved system use notification must be presented to users upon login. This notification should occur when logging into any device that provides access to CJIS data, or through each application on the device if the device itself does not present the notification.
 - The notification must include:
 - (a) A statement that the user is accessing a restricted information system.
 - (b) An advisory that system usage may be monitored, recorded, and subject to audit.
 - (c) A warning that unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
 - (d) A consent notice indicating that use of the system implies consent to monitoring and recording.
 - The system use notification message must display appropriate privacy and security notices and remain on the screen until the

803.2 STATE GOVERNMENT RECORDS ACCESS AND MANAGEMENT ACT (GRAMA)

A. Governance

- (a) **Records Section Governance:** The department's records section is governed by:
 - State Government Records Access and Management Act (GRAMA), UCA 63-2-101
 - Privacy and Security Act, Title 28
 - BCI rules and regulations

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Records Management: Access Control, GRAMA request, Data Reporting, Arrest & Warrant Records

B. Documentation

- (a) **Codes, Laws, Rules, and Regulations:** A copy of these documents is maintained by the police records manager.

C. Separation of Records

- (a) **Arrest History Files:** Separate arrest history files for adults and juveniles will be maintained in the report management system (RMS) database.

D. Juvenile Records

- (a) **Fingerprinting and Photographing:** The department will fingerprint and photograph juveniles according to Utah Rules of Juvenile Procedure 27 and UCA 78-3a-904.
- (b) **Collection, Dissemination, and Retention:** Procedures for these activities regarding juvenile records are in accordance with state and federal law.
- (c) **Expungement:** Policies and procedures for expungement of juvenile records are outlined in Utah Rules of Juvenile Procedure 56 and UCA 78-3A-904 and 78-3a-905.

E. Security and Access to Records

- (a) **Secure Area and Filing System:** The records section will maintain a secure area and filing system, allowing access to department personnel but not the general public.

F. Release of Agency Records

- (a) **Compliance with GRAMA:** Information released by the records section will comply with GRAMA and other relevant state and federal statutes and regulations.
- (b) **Active Cases:**
 - Active cases under investigation will not be released unless the requestor provides written justification to the Chief of Police or designee.
 - The Chief of Police or designee has discretion to release or withhold documents based on the request's validity.
 - **Exception:** Federal, District, or City Attorney's Office may access records if responsible for prosecuting the case.

II. RetentionA. Records Retention Schedule

- (a) **Approved Schedule:** The department's records section follows a State of Utah approved records retention schedule in compliance with applicable state statutes.

B. Records Retention Manual

- (a) **Location and Maintenance:** The records retention manual, listing retention requirements for specific records and information, is located in the records section and maintained by the records manager.

C. Review Prior to Destruction

- (a) **Review Process:**

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Records Management: Access Control, GRAMA request, Data Reporting, Arrest & Warrant Records

- Before destroying any criminal records or evidence, a review will be conducted by the Chief of Police or designee, Investigations Division Commander, and Investigations Section Sergeant.
- The review ensures that documents and items of evidence are not destroyed if they may be relevant to future investigations or inquiries.

803.2.1 CRIME DATA REPORTING

A. Uniform Crime Reporting (UCR)

- (a) **The department will participate in the Uniform Crime Reporting (UCR) program and comply with the standards set by the FBI's UCR Program; Monthly Compilation and Tri-Annual Submission:** The department compiles crime data monthly and submits it tri-annually to the Utah Division of Criminal Identification, following the guidelines in the Uniform Crime Reporting Handbook, which is retained in the records section.

B. Crime Statistics Compilation

- (a) **Monthly Data Compilation:** A crime analyst compiles crime statistics on a monthly basis.
- (b) **Tri-Annual Data Submission:** The compiled data is submitted tri-annually.

C. Release of Information

- (a) **Local Release of Information:** Information from the reports for public dissemination is handled by the department's public information officer or records supervisor with approval from the Investigative Lieutenant, Deputy Chief or Chief of Police.
- (b) **Crime Analysis Unit:** All releases of information must be compiled by the South Salt Lake City Police Department's Crime Analysis Unit and submitted to the Chief's office for review prior to final submission.
- (c) D. Uniform Crime Reporting Procedures for State and Federal mandates.

- (a) (a) **Participation in UCR System:** The South Salt Lake City Police Department participates in the statewide Uniform Crime Reporting (UCR) incident-based system through the Division of Criminal Identification.
- (b) **Monthly Totals:**
 - The NIBRS operator ensures that a monthly total of crimes, dollar loss and recovery, and arrests (as required by the state) is completed.
- (c) **Electronic Submission:** This data is submitted via computer using electronic mail to the Utah State BCI repository.
- (d) **Receipt of Reporting Results:** A copy of the UCR reporting results is received from the State on a tri-annual and annual basis.
- (b) Reports shall be submitted per requirements or mandates outlined by state and/or federal entities.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Records Management: Access Control, GRAMA request, Data Reporting, Arrest & Warrant Records

- (a) Utah's Uniform Crime Reporting Program (UCR) which uses the National Incident-Based Reporting System (NIBRS) format, including the reporting of hate crime.-UCJIS-Detective Records Tech
- (b) FBI's Law Enforcement Suicide Data Collection-UCJIS/FBI-SSLPD Crime Analyst
- (c) National Law Enforcement Accountability Database-reports of officer misconduct or criminal activity shall be report to POST per Utah Code 53-13-105-Chief of Police
- (d) FBI's National Use of Force Data Collection-UCJIS-CRB Lieutenant
- (e) FBI's Law Enforcement Officers Killed and Assaulted Data Collection-UCJIS/FBI Crime Analyst

803.2.2 ARREST REPORT, FINGERPRINTING AND PHOTOGRAPHING

A. Arrest Reports

- (a) **Documentation Requirements:**
 - All arrest reports must be completed accurately and comprehensively, detailing the circumstances of the arrest, charges, and any relevant observations or evidence.
 - Arrest reports must include personal identifying information of the arrestee, including name, date of birth, address, and any aliases.
- (b) **Timeliness:**
 - Arrest reports should be completed and submitted promptly following the arrest, ideally before the end of the officer's shift.
- (c) **Approval and Review:**
 - Completed arrest reports are reviewed and approved by a supervising officer for accuracy and completeness.
 - Any discrepancies or omissions found during the review process must be corrected immediately.
- (d) **Retention:**
 - Arrest reports are retained according to the department's approved records retention schedule and in compliance with state statutes.
- (e) **Accessibility:**
 - Arrest reports are accessible to authorized department personnel and are subject to GRAMA regulations for public access and disclosure.

B. Fingerprinting and Photographing (Adults and Juveniles)

- (a) **Adults:**
 - **Legal Basis:** Fingerprinting and photographing of adults are mandated by UCA 53-10-103 and UCA 77-7-16.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Records Management: Access Control, GRAMA request, Data Reporting, Arrest & Warrant Records

- **Procedure:**

- Adults arrested for crimes are fingerprinted and photographed during the booking process.

- Fingerprints and photographs are forwarded to the Utah Bureau of Criminal Identification (BCI).

- **Storage:** Fingerprints and photographs are stored in the department's records system and submitted to the state repository.

- (b) **Juveniles:**

- **Legal Basis:** Fingerprinting and photographing of juveniles are governed by Utah Rules of Juvenile Procedure 27 and UCA 78-3a-904.

- **Procedure:**

- Juveniles arrested for offenses that would be considered crimes if committed by adults are fingerprinted and photographed.

- Fingerprints and photographs are forwarded to the Utah BCI.

- **Storage and Confidentiality:**

- Juvenile records are maintained separately from adult records and are subject to stricter confidentiality requirements.

- Access to juvenile records is restricted to authorized personnel and in accordance with state and federal laws.

- **Expungement:**

- Juvenile fingerprint and photograph records are subject to expungement procedures outlined in Utah Rules of Juvenile Procedure 56 and UCA 78-3A-904 and 78-3a-905.

C. Security and Access to Records

- (a) **Secure Storage:**

- Fingerprint and photograph records are stored in a secure area with restricted access to ensure confidentiality and prevent unauthorized access.

- (b) **Access Restrictions:**

- Access to fingerprint and photograph records is limited to authorized personnel involved in criminal investigations, prosecutions, and record management.
- Public access to these records is regulated by GRAMA and other relevant state and federal statutes.

D. Release of Records

- (a) **Compliance with GRAMA:**

- The release of fingerprint and photograph records complies with the State Government Records Access and Management Act (GRAMA) and other applicable laws.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Records Management: Access Control, GRAMA request, Data Reporting, Arrest & Warrant Records

(b) **Public Information Officer (PIO):**

- The department's PIO manages the release of information, ensuring compliance with legal requirements and departmental policies.
- Information regarding active cases is withheld unless approved by the Chief of Police or designee based on the request's validity and necessity.

E. Training and Compliance

(a) **Personnel Training:**

- Regular training is provided to relevant personnel on the proper procedures for fingerprinting, photographing, and managing arrest records for both adults and juveniles.

(b) **Audits and Reviews:**

- Periodic audits and reviews are conducted to ensure compliance with state laws and departmental policies regarding fingerprinting, photographing, and arrest record management.

803.2.3 WARRANT AND WANTED PERSON FILES

A. Entry and Access

- (a) **Entry of Warrants:** Court clerks are responsible for entering all warrants into the statewide informational system, making them accessible through the state UCJIS files.
- (b) **NCIC Warrants:** Warrants entered into the NCIC can be accessed via the wanted person files of NCIC.
- (c) **Confirmation:** Arresting officers can confirm warrants using:
 - In-car CDPD notebook computer
 - Communications center dispatcher via the main or service channel

B. Handling of Warrants

- (a) **Use of Original and Court Copies:** Officers should use original and court copies of warrants. If necessary, a printed abstract copy can be obtained.
 - **Abstract Copies:** Available from Records division or jail personnel.
 - **Additional Copies:** Department personnel are prohibited from making additional copies of a warrant.

C. Arrest Confirmation

- **Verification:** Before making an arrest on a department warrant, the officer must verify that the original warrant is listed on the statewide warrants system.

D. Validity of Warrants

- **Expiration:** Warrants are typically valid for three years unless reissued for a longer period by the courts.

E. Procedure for Issuing Case Numbers

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Records Management: Access Control, GRAMA request, Data Reporting, Arrest & Warrant Records

- (a) **Existing Case Numbers:** Warrants related to incidents with previously assigned case numbers will retain those case numbers.
- (b) **New Case Numbers:** Warrants not related to previous incidents will be assigned a new, current case number in chronological order.
- (c) **Other Agency Warrants:** When served by department personnel:
 - Will receive a current date and case number
 - Will be designated as an agency assist
- (d) **Validation of Other Agency Warrants:** The arresting officer can validate these warrants through VECC after hours, holidays, and weekends, or through the records division during business hours (0900 to 1700, Monday through Friday).
- (e) **Post-Service Procedure:** After serving, recalling, or expiration of a warrant:
 - Communications personnel note the status on the statewide informational system.
 - Court personnel are responsible for clearing or removing the warrant.
 - All related documentation is filed in the corresponding case report file and updated in the statewide warrant system.

F. Records Maintenance

- (a) **Participation:** The South Salt Lake City Police Department, along with the South Salt Lake City Justice Court, participates in the statewide warrants system.
- (b) **Access to Records:** The appropriate courts maintain warrant records, which are accessible through VECC after hours, holidays, and weekends, or through the records division during business hours of 0900-1700 hours Monday through Friday.
- (c) **Administration:** The BCI administers the Statewide Warrants system

Restoration of Firearm Serial Numbers

804.1 PURPOSE AND SCOPE

The primary purpose for restoring firearm serial numbers is to determine the prior owners or origin of the item from which the number has been recovered. Thus, property can be returned to rightful owners or investigations can be initiated to curb illegal trade of contraband firearms. The purpose of this plan is to develop standards, methodologies and safety protocols for the recovery of obliterated serial numbers from firearms and other objects, using procedures that are accepted as industry standards in the forensic community. All personnel who are involved in the restoration of serial numbers will observe the following guidelines.

804.2 PROCEDURE

Any firearm coming into the possession of the South Salt Lake Police Department as evidence or found property, where the serial numbers have been removed or obliterated will be processed in the following manner.

804.2.1 PRELIMINARY FIREARM EXAMINATION

- (a) Always keep the muzzle pointed in a safe direction. Be sure the firearm is in an unloaded condition. This includes removal of the ammunition source (e.g., the detachable magazine, contents of the tubular magazine) as well as the chamber contents.
- (b) If the firearm is corroded shut or in a condition that would preclude inspection of the chamber contents, treat the firearm as if it is loaded. Make immediate arrangements for a firearms examiner or other qualified examiner to render the firearm safe.
- (c) Accurately record/document the condition of the gun when received. Note the positions of the various components such as the safeties, cylinder, magazine, slide, hammer. Accurately record/document cylinder chamber and magazine contents. Package the ammunition separately.
- (d) If the firearm is to be processed for fingerprints or trace evidence, process before the serial number restoration is attempted. First record/document important aspects, such as halos on the revolver cylinder face, or other relevant evidence that might be obscured by the fingerprinting chemicals.

804.2.2 PROPERTY BOOKING PROCEDURE

Any employee taking possession of a firearm with removed/obliterated serial numbers shall book the firearm into property following standard procedures. The employee booking the firearm shall indicate on the Property Form that serial numbers have been removed or obliterated.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Restoration of Firearm Serial Numbers

804.2.3 OFFICER RESPONSIBILITY

The property and evidence technician receiving a firearm when the serial numbers have been removed or obliterated shall arrange for the firearm to be examined by the Crime Scene Technician and maintain the chain of custody

804.2.4 DOCUMENTATION

Case reports are prepared in order to document the chain of custody and the initial examination and handling of evidence, from the time it was received/collected until it is released.

This report must include a record of the manner in which and/or from whom the firearm was received. This may appear on the Request Form or Property Form depending on the type of evidence.

804.2.5 FIREARM TRACE

After the serial number has been restored (or partially restored) by the criminalistics laboratory, the property and evidence technician will complete a Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) National Tracing Center (NTC) Obliterated Serial Number Trace Request Form (ATF 3312.1-OBL) and forward the form to the NTC in Falling Waters, West Virginia or enter the data into the ATF [eTrace](#) system.

804.3 OTHER CONSIDERATIONS

Exemplar bullets and cartridge cases from the firearm, depending upon acceptance criteria and protocol, may be submitted to the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), National Integrated Ballistic Information Network (NIBIN) which uses the Integrated Ballistic Identification System (IBIS) technology to digitize and compare unique markings made by a firearm on bullets and cartridge casings recovered from crime scenes.

Records Maintenance and Release

805.1 PURPOSE AND SCOPE

This policy provides guidance on the maintenance and release of [department/office] records. Protected information is separately covered in the Protected Information Policy.

805.2 POLICY

The South Salt Lake Police Department is committed to providing public access to records in a manner that is consistent with the Utah Government Records Access and Management Act (GRAMA) (Utah Code 63G-2-201 et seq.).

805.3 RECORDS OFFICER RESPONSIBILITIES

The Chief of Police shall designate a Records Officer. The responsibilities of the Records Officer include but are not limited to:

- (a) Managing the records management system for the [Department/Office], including the retention, archiving, release, and destruction of [department/office] public records.
 - 1. This includes performing the duties specified for governmental entities under GRAMA (Utah Code 63G-2-307) and the Government Data Privacy Act (Utah Code 63A-19-401 et seq.).
 - 2. This includes the maintenance and destruction of imaging surveillance data as required by Utah Code 77-23d-105.
- (b) Maintaining and updating the [department/office] records retention schedule including:
 - 1. Identifying the minimum length of time the [Department/Office] must keep records.
 - 2. Identifying the division responsible for the original record.
- (c) Establishing rules regarding the inspection and copying of [department/office] public records as reasonably necessary for the protection of such records.
- (d) Identifying records or portions of records that are confidential under state or federal law and not open for inspection or copying.
 - 1. The Records Officer shall be responsible for filing a statement with the state archivist explaining the reasons a record series that is designated as private or controlled under GRAMA is being collected or used by the [Department/Office] (Utah Code 63G-2-601).
- (e) Establishing rules regarding the processing of subpoenas for the production of records.
- (f) Ensuring a current schedule of fees for public records as allowed by law is available (Utah Code 63G-2-203).
- (g) Forwarding requests to the appropriate agency when a requester seeks records that are not in the possession of the [Department/Office] (Utah Code 63G-2-204).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Records Maintenance and Release

805.4 PROCESSING REQUESTS FOR PUBLIC RECORDS

Any [department/office] member who receives a request for any record shall route the request to the Records Officer or the authorized designee.

805.4.1 REQUESTS FOR RECORDS

The processing of requests for any record is subject to the following:

- (a) The [Department/Office] is not required to create records that do not exist.
- (b) When a record contains material with release restrictions and material that is not subject to release restrictions, the restricted material shall be redacted and the unrestricted material released.
 - 1. A copy of the redacted release should be maintained in the case file for proof of what was actually released and as a place to document the reasons for the redactions. If the record is audio/video, a copy of the redacted audio/video release should be maintained in the [department/office]-approved media storage system and a notation should be made in the case file to document the release and the reasons for the redacted portions.
- (c) Requests for records must be in writing and contain the requester's name, contact information, and a description of the record requested (Utah Code 63G-2-204).
- (d) The Records Officer shall review each request for records within 10 business days unless the person has requested an expedited response. Expedited requests must be reviewed within five business days (Utah Code 63G-2-204).
- (e) Unless the Records Officer is prohibited by law from releasing the requested record, or extraordinary circumstances, as defined in Utah Code 63G-2-204, or other exception exists, the record shall be released (Utah Code 63G-2-201).
 - 1. If the existence of extraordinary circumstances precludes approval or denial of the request within the time permitted under law, additional time may be granted.
 - 2. A request made by or on behalf of a person on parole, or in jail or another correctional facility following a conviction, may be denied unless it is submitted by an attorney of that person or is one of their first five requests submitted during a calendar year requesting only a record that contains a specific reference to that person (Utah Code 63G-2-201).
- (f) If the Records Officer denies a request, a notice of denial shall be sent to the requester. The notice shall contain a description of the record denied, the legal basis upon which the Records Officer relied in denying the request, and information related to the appeal process available to the requester (Utah Code 63G-2-205).

805.4.2 APPEALS

The denial of a request for records or a fee waiver by the Records Officer may be appealed to the Chief of Police (Utah Code 63G-2-401). Upon receipt of a notice to appeal, the Chief of Police must review and make a determination within 10 business days (or five business days if the requester or interested party demonstrates that an expedited decision benefits the public). If a determination is not made within the specified time frame, the appeal shall be considered denied.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Records Maintenance and Release

If the Chief of Police affirms the denial, notice shall be sent to the requester informing them of (Utah Code 63G-2-401):

- (a) The right to request that the government records ombudsman mediate the dispute.
- (b) The right to appeal the denial to the director of the Government Records Office, the district court, or the local appeals board, if established.
- (c) The time limits for filing such mediation request and appeal.
- (d) The contact information of the executive secretary of the records committee, local appeals board, if established, and the government records ombudsman.

805.5 RELEASE RESTRICTIONS

Examples of release restrictions include:

- (a) Any personal identifying information, including an individual's photograph; Social Security and driver identification numbers; name, address and telephone number; and medical or disability information that is contained in any driver license record, motor vehicle record or any [department/office] record, including traffic accident reports, are restricted except as authorized by the [Department/Office], and only when such use or disclosure is permitted or required by law to carry out a legitimate law enforcement purpose (18 USC § 2721; 18 USC § 2722; Utah Code 53-3-109; Utah Code 41-6a-404).
- (b) Victim information that may be protected by statutes (Utah Code 77-37-4).
- (c) Personnel records (Utah Code 63G-2-302; Utah Code 63G-2-303).
 - 1. Specific personnel information related to undercover officers or investigative personnel is exempt from disclosure if release could reasonably impair the effectiveness of investigations or endanger any individual's safety (Utah Code 63G-2-301).
- (d) Properly classified records that contain medical, psychiatric, or psychological data about a person if release would be detrimental to the person's mental health or safety, or would violate normal professional practice and medical ethics (Utah Code 63G-2-304).
- (e) Records created exclusively in anticipation of potential litigation involving this [department/office] (Utah Code 63G-2-305).
- (f) Automated license plate reader (ALPR) data (Utah Code 41-6a-2004).
- (g) Imaging surveillance data (Utah Code 77-23d-105).
- (h) Certain types of reports involving but not limited to child abuse and neglect (Utah Code 80-2-1005).
- (i) Certain audio and video recordings created by a body-worn camera that recorded sound or images:
 - 1. Inside a home or residence (Utah Code 63G-2-302; Utah Code 77-7a-107).
 - 2. Inside a hospital or health care facility, inside a clinic of a health care provider, or inside a human service program (Utah Code 63G-2-305).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Records Maintenance and Release

- (j) Certain data collected by an unmanned aerial system (Utah Code 72-10-803).
- (k) Data, other than certain statistical information, relating to facial recognition comparisons conducted against a government image database (Utah Code 77-23e-106).
- (l) Any other information that may be appropriately denied by:
 - 1. Utah Code 63G-2-302 (private records).
 - 2. Utah Code 63G-2-303 (private information of government employees).
 - 3. Utah Code 63G-2-304 (controlled records).
 - 4. Utah Code 63G-2-305 (protected records).

805.6 SUBPOENAS AND DISCOVERY REQUESTS

Any member who receives a subpoena duces tecum or discovery request for records should promptly contact a supervisor and the Records Officer for review and processing. While a subpoena duces tecum may ultimately be subject to compliance, it is not an order from the court that will automatically require the release of the requested information.

Generally, discovery requests and subpoenas from criminal defendants and their authorized representatives (including attorneys) should be referred to the District Attorney, City Attorney, or the courts.

All questions regarding compliance with any subpoena duces tecum or discovery request should be promptly referred to legal counsel for the [Department/Office] so that a timely response can be prepared.

805.7 RELEASED RECORDS TO BE MARKED

Each page of any written record released pursuant to this policy should be stamped in a colored ink or otherwise marked to indicate the [department/office] name and to whom the record was released.

Each audio/video recording released should include the [department/office] name and to whom the record was released.

805.8 EXPUNGEMENT

Expungement orders received by the [Department/Office] shall be reviewed for appropriate action by the Records Officer. The Records Officer shall expunge such records as ordered by the court. Records may include but are not limited to a record of arrest, investigation, detention, or conviction. Once expunged, members shall respond to any inquiry as though the record did not exist.

The Records Officer shall provide written confirmation that all records have been expunged by the [Department/Office] to the individual receiving the expungement if requested (Utah Code 77-40a-401).

Upon receiving an order for vacatur, the Records Officer shall comply with the provisions of Utah Code 77-40a-402.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Records Maintenance and Release

805.9 RELEASE OF RECORDINGS RELATED TO CRITICAL INCIDENTS

Video and audio recordings of incidents made by officers of this [department/office] that resulted in death or serious bodily injury of an individual or during which an officer fired a weapon shall be released upon receipt of a proper public records request.

The Records Officer should coordinate as appropriate with the Chief of Police or the prosecuting agency to determine which recordings may qualify for disclosure when a request for a recording is received (Utah Code 77-7a-107).

805.10 DATA SECURITY

Members who become aware that any [department/office] system containing personal information may have been breached should notify the Records Officer as soon as practicable.

If a data breach occurs, the Utah Cyber Center and Attorney General should be notified, and an internal incident report should be prepared, when required by Utah Code 63A-19-405. Notice should be provided to individuals affected by the data breach when appropriate pursuant to Utah Code 63A-19-406.

805.11 TRAINING

The Records Supervisor shall, on an annual basis, successfully complete an online records management training course provided by the Utah Department of Administrative Services' Division of Archives and Records Service (Utah Code 63G-2-108).

Protected Information

806.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the access, transmission, release, and security of protected information by members of the South Salt Lake Police Department. This policy addresses the protected information that is used in the day-to-day operation of the [Department/Office] and not the public records information covered in the Records Maintenance and Release Policy.

806.1.1 DEFINITIONS

Definitions related to this policy include:

Protected information - Any information or data that is collected, stored or accessed by members of the South Salt Lake Police Department and is subject to any access or release restrictions imposed by law, regulation, order or use agreement. This includes all information contained in federal, state or local law enforcement databases that is not accessible to the public.

Director of Bureau-Director of the Bureau of Criminal Identification

Commissioner-Commissioner of Public Safety

806.2 POLICY

Members of the South Salt Lake Police Department will adhere to all applicable laws, orders, regulations, use agreements and training related to the access, use, dissemination and release of protected information.

806.3 RESPONSIBILITIES

The Chief of Police shall select a member of the [Department/Office] to coordinate the use of protected information.

The responsibilities of this position include but are not limited to:

- (a) Ensuring member compliance with this policy and with requirements applicable to protected information, including requirements for the National Crime Information Center (NCIC) system, National Law Enforcement Telecommunications System (NLETS), Department of Motor Vehicle (DMV) records, and the Utah Criminal Justice Information System (UCJIS).
- (b) Developing, disseminating, and maintaining procedures that adopt or comply with the U.S. Department of Justice's current Criminal Justice Information Services (CJIS) Security Policy. See the South Salt Lake Police Department CJIS Access, Maintenance, and Security Policy for additional guidance.
- (c) Developing, disseminating, and maintaining any other procedures necessary to comply with any other requirements for the access, use, dissemination, release, and security of protected information.
- (d) Developing procedures to ensure training and certification requirements are met.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Protected Information

- (e) Resolving specific questions that arise regarding authorized recipients of protected information.
- (f) Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

806.4 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, South Salt Lake Police Department policy, or training. Only those members who have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the member has a legitimate work-related reason for such access.

Unauthorized access, including access for other than a legitimate work-related purpose, is prohibited and may subject a member to administrative action pursuant to the Personnel Complaints Policy and/or criminal prosecution. See the CJIS Access, Maintenance, and Security Policy for additional guidance.

806.4.1 PENALTIES FOR MISUSE OF RECORDS

Misuse of access to criminal history record information is a class B misdemeanor (Utah Code 53-10-108).

Divulging the content of any criminal record to anyone other than authorized personnel is a violation of the Standards of Conduct Policy.

Employees who obtain, or attempt to obtain, information from the [department/office] files other than that to which they are entitled in accordance with their official duties is a violation of the Standards of Conduct Policy.

806.4.2 RELEASE OF CHRI

Only the persons listed below are authorized to release CHRI. Each authorized person releasing CHRI is responsible to ensure that each request granted appears legitimate and that the requester is an authorized recipient with a right and need to know.

- (a) Criminal Records Security Officer.
- (b) Records Supervisor.
- (c) Full-time employees of the Records Section.
- (d) Personnel specifically designated in writing by Division Commanders with the concurrence of the Criminal Records Security Officer.

806.5 RELEASE OR DISSEMINATION OF PROTECTED INFORMATION

Protected information may be released only to authorized recipients who have both a right to know and a need to know (Utah Code 53-10-108).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Protected Information

A member who is asked to release protected information that should not be released should refer the requesting person to a supervisor or to the Records Supervisor for information regarding a formal request.

Unless otherwise ordered or when an investigation would be jeopardized, protected information maintained by the [Department/Office] may generally be shared with authorized persons from other law enforcement agencies who are assisting in the investigation or conducting a related investigation. Any such information should be released through the Records Section to ensure proper documentation of the release (see the Records Maintenance and Release Policy).

Protected information, such as Criminal Justice Information (CJI), which includes Criminal History Record Information (CHRI), should generally not be transmitted by radio, cellular telephone, or any other type of wireless transmission to members in the field or in vehicles through any computer or electronic device, except in cases where there is an immediate need for the information to further an investigation or where circumstances reasonably indicate that the immediate safety of officers, other [department/office] members or the public is at risk.

Nothing in this policy is intended to prohibit broadcasting warrant information.

806.6 SECURITY OF PROTECTED INFORMATION

The Chief of Police will select a member of the [Department/Office] to oversee the security of protected information.

The responsibilities of this position include but are not limited to (see the CJIS Access, Maintenance, and Security Policy for additional guidance):

- (a) Developing and maintaining security practices, procedures, and training.
- (b) Ensuring federal and state compliance with the CJIS Security Policy and the requirements of any state or local criminal history records systems.
- (c) Establishing procedures to provide for the preparation, prevention, detection, analysis, and containment of security incidents, including computer attacks.
- (d) Tracking, documenting, and reporting all breach of security incidents to the Chief of Police and appropriate authorities (Utah Code 63A-19-405; Utah Code 63A-19-406).
- (e) Developing procedures and ensuring compliance with the Government Data Privacy Act (Utah Code 63A-19-401 et seq.).

806.6.1 MEMBER RESPONSIBILITIES

Members accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized to access or receive it. This includes leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (e.g., on an unattended table or desk; in or on an unattended vehicle; in an unlocked desk drawer or file cabinet; on an unattended computer terminal).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Protected Information

806.6.2 INTIMATE IMAGES

Any member who obtains access to an intimate image (as defined in Utah Code 76-5b-203) in the course of a criminal action shall not display, duplicate, copy, or share the intimate image unless the member is doing so solely for the purpose of the adjudication, defense, prosecution, or investigation of a criminal matter involving the intimate image as required by state law (Utah Code 76-5b-203.5). Any such disclosure of an intimate image requires supervisory approval.

806.7 PERSONALLY IDENTIFIABLE INFORMATION-PII

1. PII shall be collected only when the Agency has the legal authority to do so and the PII is necessary to the conduct of official duties.

a. Limit Use: Access PII only when the information is needed in the conduct of your official duties. PII is to be utilized for official purposes only. PII shall not be utilized for personal reasons.

b. Limit proliferation: Do not create unnecessary or duplicative collections of PII. If you need to create duplicate copies of documents containing PII to perform your duties then delete or destroy them when they are no longer needed. Unauthorized replication, especially for personal use, may constitute a violation of policy. When you need to print, copy, or extract PII from documents, target only the PII that is required for the task at hand.\

2. The following measures shall be taken to ensure the protection of PII:

a. Any mobile computer, mobile computing device or removable storage media that processes, stores, or transmits electronic records containing PII shall store and transmit that data encrypted. That encryption shall conform to 140-2FIPS-CERTIFIED, National Institute of Technologies (NIST) standards specified in the CJI Information Handling section (MINIMALLY OR CURRENT). User authentication providing access to said data shall be via an authorized advanced authentication mechanism or passwords as specified in the Information Security Policy. Approved software for file and folder encryption is available from a request from IT and coordination with a records technician.[NIST-Computer Security Resource Center](#)

b. Storage of PII shall be restricted to agency-owned devices. PII shall not be stored or transmitted via personally owned devices including but not limited to computers, cellphones, flash drives, CDs, and DVDs.

c. Do not take PII home or to any unsecured worksite in either paper or electronic form unless appropriately secured. PII in electronic form must be encrypted as specified above.

d. When emailing PII to any recipient not covered by an agency agreement or transmitted via an unsecured network then PII must be sent via an encrypted attachment with the password provided separately (e.g. by phone or in person).

e. Do not leave PII unattended in any unsecured space where it might be accessed by unauthorized persons.

f. Store PII in shared access computer drives ("shared folders") only if access to those folders is restricted to those with a need to know by access permissions.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Protected Information

- g. Physically secure PII when in transit. Do not mail or courier PII on media unless the data is encrypted.
- h. Protect PII data during all stages of its life cycle. Do not discard or provide any vendor for maintenance media holding PII.
- i. Do not place laptops or removable media in checked baggage. Do not leave them in an unsecured car overnight or unsecured in plain sight in public places.
- j. If you are sent unsecured PII you still must secure it once you receive it.
- k. Adhere to all provisions of Information Systems and Security Policies. <https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center>

806.8 TRAINING

All members authorized to access or release protected information shall complete a training program that complies with any protected information system requirements and identifies authorized access and use of protected information, as well as its proper handling and dissemination.

806.8.1 COMPUTER TERMINAL SECURITY

Computer terminal equipment capable of providing access to automated criminal offender record information is located in the Records Section, Dispatch and in the Investigations Division to preclude access by unauthorized persons.

No employee shall be authorized to operate computer terminal equipment with access to CHRI until the operator has completed the appropriate training.

806.8.2 DESTRUCTION OF CHRI

When any document providing CHRI has served the purpose for which it was obtained, it shall be destroyed by shredding.

Each employee shall be responsible for destroying the CHRI documents they receive.

806.8.3 DATA PRIVACY TRAINING

All members with access to personal data retained by the [Department/Office] shall complete data privacy training within 30 days of beginning employment and annually thereafter (Utah Code 63A-19-401.2).

Computers and Digital Evidence

807.1 PURPOSE AND SCOPE

This policy establishes procedures for the seizure and storage of computers, personal communications devices (PCDs) digital cameras, digital recorders and other electronic devices that are capable of storing digital information; and for the preservation and storage of digital evidence. All evidence seized and/or processed pursuant to this policy shall be done so in compliance with clearly established Fourth Amendment and search and seizure provisions.

807.2 SEIZING COMPUTERS AND RELATED EVIDENCE

Computer equipment requires specialized training and handling to preserve its value as evidence. Officers should be aware of the potential to destroy information through careless or improper handling, and therefore they should utilize the most knowledgeable available resources. When possible, this includes enlisting the help of a computer forensics examiner, who will make an exact copy, or mirror image, of the computer's hard drive; the original will be stored as evidence. This eliminates the possibility of altering or destroying any evidence on the original. The examiner will then search the copy of the hard drive for evidence.

When seizing a computer and accessories the following steps should be taken:

- (a) Photograph each item, front and back, specifically including cable connections to other items. Look for a phone line or cable to a modem for Internet access.
- (b) Do not overlook the possibility of the presence of physical evidence on and around the hardware relevant to the particular investigation such as fingerprints, biological or trace evidence and/or documents.
- (c) If the computer is off, do not turn it on.
- (d) If the computer is on, do not shut it down normally and do not click on anything or examine any files.
 1. Photograph the screen, if possible, and note any programs or windows that appear to be open and running.
 2. Disconnect the power cable from the back of the computer box or if a portable notebook style, disconnect any power cable from the case and remove the battery.
- (e) Label each item with case number, evidence sheet number, and item number.
- (f) Handle and transport the computer and storage media (e.g., tape, discs, memory cards, flash memory, external drives) with care so that potential evidence is not lost.
- (g) Lodge all computer items in the Property Room. Do not store computers where normal room temperature and humidity is not maintained.
- (h) At minimum, officers should document the following in related reports:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Computers and Digital Evidence

1. Where the computer was located and whether it was in operation.
 2. Who was using it at the time.
 3. Who claimed ownership.
 4. If it can be determined, how it was being used.
- (i) In most cases when a computer is involved in criminal acts and is in the possession of the suspect, the computer itself and all storage devices (hard drives, tape drives and disk drives) should be seized along with all media. Accessories (printers, monitors, mouse, scanner, keyboard, cables, software and manuals) should not be seized unless as a precursor to forfeiture.

807.2.1 BUSINESS OR NETWORKED COMPUTERS

If the computer belongs to a business or is part of a network, it may not be feasible to seize the entire computer. Cases involving networks require specialized handling. Officers should contact a certified forensic computer examiner for instructions or a response to the scene. It may be possible to perform an on-site inspection, or to image the hard drive only of the involved computer. This should only be done by someone specifically trained in processing computers for evidence.

807.2.2 FORENSIC EXAMINATION OF COMPUTERS

If an examination of the contents of the computer's hard drive, floppy disks, compact discs or any other storage media is required, an exact duplicate of the hard drive or disk will be made using a forensic computer and a forensic software program by someone trained in the examination of computer storage devices. The officer will then forward the following items to a computer forensic examiner:

- (a) Copy of report(s) detailing how the computer was used in criminal activities. Also include the Evidence/Property sheet.
- (b) Copy of a consent to search form signed by the computer owner or the person in possession of the computer, or a copy of a search warrant authorizing the search of the computer hard drive for evidence relating to the investigation.
- (c) A listing of the items to search for (e.g., photographs, financial records, e-mail, documents).
- (d) An exact duplicate of the hard drive or disk will be made using a forensic computer and a forensic software program by someone trained in the examination of computer storage devices for evidence.

807.3 SEIZING DIGITAL STORAGE MEDIA

Digital storage media including hard drives, floppy discs, CDs, DVDs, tapes, memory cards or flash memory devices should be seized and stored in a manner that will protect them from damage.

- (a) If the media has a write-protection tab or switch, it should be activated.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Computers and Digital Evidence

- (b) Do not review, access or open digital files prior to submission to a computer forensic examiner. If the information is needed for immediate investigation request the Evidence Room to copy the contents to an appropriate form of storage media.
- (c) Many kinds of storage media can be erased or damaged by magnetic fields. Keep all media away from magnetic devices, electric motors, radio transmitters or other sources of magnetic fields.
- (d) Do not leave storage media where it would be subject to excessive heat, such as in a parked vehicle on a hot day.
- (e) Use plastic cases designed to protect the media, or other protective packaging, to prevent damage.

807.4 SEIZING PCDS

Personal communication devices (PCDs) such as cell phones, Personal Digital Assistants (PDAs) or other hand-held devices connected to any communication network must be handled with care to preserve evidence that may be on the device, which includes messages, stored data and/or images.

- (a) Officers should not attempt to access, review or search the contents of such devices prior to examination by a forensic expert. Un-sent messages can be lost, data can be inadvertently deleted and incoming messages can override stored messages.
- (b) When seizing the devices, also seize the charging units and keep them plugged in to the chargers until the devices can be examined. If the batteries go dead all the data may be lost.

807.5 DIGITAL EVIDENCE RECORDED BY OFFICERS

Officers handling and submitting recorded and digitally stored evidence from digital cameras and audio or video recorders will comply with these procedures to ensure the integrity and admissibility of such evidence.

807.5.1 COLLECTION OF DIGITAL EVIDENCE

Once evidence is recorded it shall not be erased, deleted or altered in any way prior to submission. All photographs taken will be preserved regardless of quality, composition or relevance. Video and audio files will not be altered in any way.

807.5.2 SUBMISSION OF DIGITAL MEDIA

The following are required procedures for the submission of digital media used by cameras or other recorders:

- (a) The recording media (smart card, compact flash card or any other media) shall be brought to the Evidence Room as soon as possible for submission into evidence.
- (b) Officers are not authorized to review or copy memory cards. The evidence technicians are the only employees authorized to copy and/or distribute digital media made from the memory cards.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Computers and Digital Evidence

807.5.3 DOWNLOADING OF DIGITAL FILES

Digital information such as video or audio files recorded on devices using internal memory must be downloaded to storage media. The following procedures are to be followed:

- (a) Files should not be opened or reviewed prior to downloading and storage.
- (b) Where possible, the device should be connected to a computer and the files accessed directly from the computer directory or downloaded to a folder on the host computer for copying to the storage media.

807.5.4 PRESERVATION OF DIGITAL EVIDENCE

- (a) Only evidence technicians are authorized to copy original digital media that is held as evidence. The original digital media shall remain in evidence and shall remain unaltered.
- (b) Digital images that are enhanced to provide a better quality photograph for identification and investigative purposes must only be made from a copy of the original media.
- (c) If any enhancement is done to the copy of the original, it shall be noted in the corresponding incident report.

Cash Control of Investigative Funds, Petty Cash, Receipts

808.1 POLICY

- (a) The South Salt Lake Police Department limits actual cash collection to those funds seized in the course of criminal investigations only.
- (b) Disbursement of cash is strictly safeguarded and is limited to "Investigative Funds", "Petty Cash" and "Cash Receipts"
- (c) Disbursement of VOCA grant's "Other Emergency Funds" is strictly safeguarded and is limited to expenditures on behalf of violent crime victims for emergency needs.
- (d) Preparation of financial statements, internal audits, and related matters are governed by procedures of the South Salt Lake City Financial Department.
 - 1. Frequency of audits of specified police department funds are as follows:
 - (a) Investigative/Informant and Petty Cash Funds are audited at least semi-annually by the Chief of Police or his/her designee.
 - (b) Investigative/Informant and Petty Cash Funds are audited at least semi-annually by the City Finance Department.
 - (c) Investigative/Informant Funds will be accounted for by the Investigations Division Commander tri-annually.
 - 1. The results of the accounting shall be forwarded via memorandum to the Chief of Police or his/her designee.
 - (d) Evidence/Property Funds are audited at least annually by the City Finance Department.
 - 1. This audit will be conducted in the presence of a member of the Evidence/ Property room in order to maintain the chain of custody.
 - 2. VOCA's "Other Emergency Funds" will be strictly accounted for by the South Salt Lake City Finance Department. Accounting logs will be provided quarterly to the Finance Department. As awarded funds are expended, these amounts will also be provided to the police chief's administrative assistant.

808.1.1 PROCEDURES

- (a) Investigative Funds distribution will occur as follows:
 - 1. The Investigations Division Commander will issue all investigative funds to the Investigations Section Sergeant.
 - (a) The funds will be issued by use of a receipt, signed by the commander and sergeant.
 - (b) The commander will retain the original receipt and provide a copy to the sergeant.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Cash Control of Investigative Funds, Petty Cash, Receipts

2. The Investigations Section Sergeant will issue the funds to the appropriate investigator/officer for a specific assignment.
 - (a) The same receipt procedure will take place between the sergeant and investigator/ officer.
 3. At the completion of the assignment and/or the end of the month, the investigator/officer will return to the sergeant any unexpended funds and/or a log containing the following information:
 - (a) Date and time of the expenditure of the funds.
 - (b) Amount of expenditure.
 - (c) Who received the funds and for what purpose.
 - (d) Case number associated with the particular expenditure.
 - (e) If at all possible a signature from the person(s) receiving the funds should be obtained on a receipt.
 1. In cases where it is important to maintain an officers undercover identity, a signature is not required.
 4. No later than the 5th day of the following month, the Investigations Section Sergeant will forward all copies of all receipts and the investigator's log to the Investigations Division Commander, in conjunction with the sections end of month reports.
 5. Expenditures in excess of \$200 dollars for informant pay, or for a single drug transactions in excess of \$500 dollars, require pre-approval of the Investigations Division Commander.
 - (a) Any expenditure over \$1,000 dollars requires approval from the Chief of Police or designee.
- (b) Procedures for money obtained via legal process are as follows:
1. Money seized pursuant to a search warrant is processed according to current case law, pertinent department policies and court rulings.
 2. All monies are to be accounted for by denomination and, if necessary, serial number.
 3. All monies are to be noted on department evidence forms and reports, refer to South Salt Lake Police Policy and Procedure, Chapter 34 (I), (A), (e), (i) and (ii).
 4. Any forfeited monies become the property of the City of South Salt Lake and shall be periodically audited according to City and Department policy.
- (c) Procedures for petty cash handling are as follows:
1. The Chief of Police or his/her designee and the Executive Secretary will be the only person(s) authorized to receive and disburse petty cash funds.
 2. Signed receipts of the payment to the requestor will be documented on all petty cash fund disbursements.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Cash Control of Investigative Funds, Petty Cash, Receipts

3. At least tri-annually, the Chief of Police or his/her designee will account for the activity of the petty cash fund.
 4. All funds within the Department are subject to random inspections.
- (d) Cash Receipts:
1. Absolutely no unauthorized persons shall touch the cash drawer/till.
 2. Only authorized personnel may handle cash, credit cards or checks for cash receipts.
 3. The cash receipt drawer/till must be balanced daily and deposits taken to the Finance Department no later than 12:00 hours daily.
 4. Any cash, checks or credit card information is to be locked in a safe after hours or when unattended.
 5. There is never to be cash given back on checks that are written over the amount needed. If needed, a check request can be written for the excess amount and mailed out to the recipient.
 6. No cashing checks for cash back, not even for employees.
 7. Checks are not to be held for any reason. Correct dates should be on the check when received and deposited immediately.
- (e) Cash Receipt Procedures:
1. When opening the cash receipts program, check to make sure you are on the current date, you will have to manually change the date if necessary.
 2. When adding information in the Payment Entry, accuracy is very important.
 - (a) Add any extra information in the description box that you have, including the name and purpose of payment.
 - (b) Be sure that the Distribution Code and G. L. account number is correct.
 - (c) Verify the correct distribution amount and the type of payment (cash, check, money order or credit) used.
 - (d) If the name on a check is different than the receipt, indicate that in the "Payer box".
 - (e) Include the check or money order number in the space provided, and if paying by credit card, use the first 4 and the last 4 numbers of the card.
 - (f) Verify the payment amount and cash back, if any.
 - (g) There is never to be cash back distributed from a check or credit card transaction.

808.2 PROCEDURES

A. VOCA Grant's "Other Emergency Funds" distribution will occur as follows:

1. The Victim Services Supervisor will request grant awarded funding through the Chief's Office.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Cash Control of Investigative Funds, Petty Cash, Receipts

2. Prior to funds being issued, all previously issued "other emergency funds" will have been accounted for by the Victim Services Supervisor submitting a detailed accounting to the Chief's Office.
3. The Victim Services Supervisor will maintain all accounting logs for a period of three years, which is required for VOCA grant funding.
4. The accounting roster will be provided to the Finance Office, along with the quarterly grant reimbursement request ledger.

Multi-Jurisdictional Communications Agreement

809.1 PURPOSE AND SCOPE

The South Salt Lake City Police Department utilizes the services of the Valley Emergency Communications Center (VECC) for all of its dispatching needs. VECC and the South Salt Lake City Police Department maintain an alliance that will provide compliance with the standards set forth in this chapter. The VECC, as well as department employees, shall comply with all Federal Communications Commission (FCC) standards and procedures.

809.1.1 RESOURCES AVAILABLE

- (a) VECC personnel have access to the following information concerning the South Salt Lake City Police Department:
 - 1. Officer in charge.
 - 2. Duty roster on each shift.
 - 3. Residential telephone numbers of every agency member.
 - 4. Visual maps detailing the agency's service area.
 - 5. Officer status indicators.
 - 6. Written procedures and telephone numbers for procuring emergency and necessary external services to the agency.
 - 7. Tactical dispatching plans.
 - 8. Off-duty officer contact information:
 - (a) Should communications personnel need to contact off-duty South Salt Lake City Police Department personnel, they will contact the off-duty officer at home, using the home phone number list supplied to the communications center by the South Salt Lake City Police Department.
 - (b) When an off-duty officer cannot be reached at home, the communications center will contact the officer's cell phone, if the off-duty officer is so equipped.
 - 9. Maps or other visual representations that detail the agency's service area
 - (a) This is to help VECC personnel properly identify a caller's location, determine agency jurisdiction, and dispatch the appropriate field units.
- (b) Officer Status Indicators:
 - (a) Officer status indicators are visually available to each communications operator and are important because they allow the communications operator to know the status of every officer under his/her control.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Multi-Jurisdictional Communications Agreement

- (b) Officers depend on the communications center to recognize when they might be in danger by monitoring the officer status indicators.
- (c) The communications operators know where and how long each officer has been out on a call, as well as, know which car is available for a call.
- (c) Procurement of External Services:
 - (a) On occasion, situations arise requiring additional resources. Officers may request resources by contacting the VECC. The external services include, but are not limited to:
 - (a) Fire apparatus.
 - (b) Environmental services.
 - (c) Human services.
 - (d) Ambulances / Paramedics / Emergency Medical Technicians (EMTs).
 - (e) Air Ambulances.
 - (f) Wreckers.
 - (g) Other services that are not components of the South Salt Lake City Police Department.
 - (b) The VECC shall maintain the necessary information on external services for the South Salt Lake City Police Department. The procedures must be specific for each individual service in order to provide prompt assistance in all situations, especially emergencies.
- (d) Tactical dispatching plans:
 - 1. The VECC shall provide access and training to their employees in the area of tactical dispatching plans. South Salt Lake police tactical plans are available to VECC employees in the VECC operational handbook. These plans may include, but are not limited to:
 - (a) Bank robbery.
 - (b) Tactical team.
 - (c) Pursuit.
 - (d) Mutual aid.
 - (e) Police service dog.
- (e) Emergency service agencies telephone numbers:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Multi-Jurisdictional Communications Agreement

- (a) Employees of the VECC shall have available to them by means of a private line, telephone index, book, or other means, the telephone numbers of emergency service agencies to expedite contacting the following agencies:
 - (a) Fire agencies.
 - (b) Rescue agencies.
 - (c) Life squad units.
 - (d) Animal control units.
 - (e) Tactical teams.
 - (f) Medical agencies.
- (f) Accessibility to radio communications:
 - 1. Officers shall maintain radio contact with the VECC and be available to respond to emergency calls while on-duty, or off-duty while operating a police vehicle, except when previously authorized to be out-of-service.
 - 2. When in police vehicles, off-duty officers must keep the radio on and, if necessary, be available to respond to emergency calls.

809.1.2 RECORDING COMMUNICATIONS

- (a) The VECC shall record all radio transmissions and all emergency telephone conversations within the communications center.
 - 1. These records are an indispensable source for criminal investigations, internal investigations, training, and audits of the South Salt Lake City Police Department service delivery system.
 - 2. The VECC shall retain recorded tapes for a minimum of thirty-days (30).
 - 3. Recordings will be handled and stored in a secured area.
- (b) Reviewing Audio Recordings:
 - 1. Access to audio recordings shall be limited to:
 - (a) The VECC personnel.
 - (b) The personnel of the South Salt Lake City Police Department, when the need for a recording exists.
 - 2. If an officer believes that he/she has a need to listen to radio or telephone conversations, or make a copy of the same, he/she shall:
 - (a) Determine if a need exists. Need includes, but is not limited to criminal investigation, internal investigation, training matters, or audit on how South

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Multi-Jurisdictional Communications Agreement

Salt Lake City Police Department personnel conducted themselves on radio or telephone lines.

- (b) Contact his/her supervisor.
 - (c) Should the officer's supervisor agree that the need exists to listen to and/or record a conversation, he/she shall have the officer complete a VECC Tape Request Form and obtain the watch commander's signature. The form will then be forwarded to the administrative officer, who will notify the VECC supervisor and request that a copy of the pertinent audio recordings be produced.
 - (d) The administrative officer shall provide the VECC the date, time, nature of the incident, and whether it was a radio or telephone conversation, to help locate the needed recording(s).
- 3. Persons who have access to the telephone and radio audio recordings shall be familiar with the playback requirements and appropriate documentation. Proper care must be exercised to assure that recordings are not accidentally erased.
 - 4. Attorneys who request copies of an audio recording shall be advised that they must make the request via subpoena.
 - 5. Members of the media who request copies of an audio recording shall be advised that their request must be reviewed and approved by the Chief of Police prior to the release of the information.
 - 6. Immediate playback:
 - (a) An emergency caller or an officer may not be able to repeat information. VECC personnel have the ability to instantly replay a telephone or radio conversation, in the event that the original audio was not clear.

809.1.3 PARTICIPATION IN INFORMATION SYSTEMS

- (a) The effectiveness of investigative efforts depends heavily upon the quality of information resources. The VECC has access to local, state, and federal criminal justice information for use by authorized personnel only.
 - 1. The South Salt Lake City Police Department participates in the centralized, statewide criminal identification system through the Division of Criminal Identification (BCI).
 - 2. The South Salt Lake City Police Department maintains, through agreement with the State of Utah, computer access to the state's criminal information files and various states' driver license and vehicle registration databases, criminal history systems, NCIC, and other data sources allowed by law.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Multi-Jurisdictional Communications Agreement

3. All stolen property, missing persons, and other information allowed by BCI and access policy will be entered according to proper procedures.
 4. The access terminal allows point-to-point (teletype) communication between this department and other local and national users.
- (b) Use of the system and the information obtained is limited to law enforcement personnel only.
1. No private party or non-governmental agency shall be provided information or allowed to utilize this system.
 2. Non-departmentally sanctioned, private use of department employees is prohibited.

809.1.4 CRITERIA FOR EMERGENCY MESSAGES

- (a) Delivering emergency messages is a legitimate law enforcement function. When VECC personnel receive information that indicates the need for the delivery of an emergency message, they will notify the agency with jurisdiction. The South Salt Lake City Police Department personnel will deliver emergency messages when any of the following conditions are present:
1. Notification of next of kin in the event of death or medical emergency.
 2. Notification to a person to make an emergency phone call concerning a death or medical emergency.
 3. Notification of next of kin in the event of a traffic accident.
 4. Notification of a person in regards to another person being stranded.
 5. Notification of individuals required by the Spouse Abuse Act.
 6. Any other situation in which the shift supervisor or duty officer feels there is justification to deliver an emergency message.
- (b) Officers shall respond to the proper address and deliver the message in an accurate, conscientious, and professional manner.
- (c) When officers request VECC to telephonically contact a person, the dispatcher shall do so accordingly, and notify the officer whether the message was given or that there was no contact made.
- (d) Dispatchers may also access the services of the Department Chaplains or victim advocates, if requested by the on-duty supervisor.

Pharmaceutical Drug Collection Program

810.1 PURPOSE AND SCOPE

The purpose of this policy is to establish procedures for collection, documentation, handling and destruction of collected controlled substances and for implementing prevention strategies.

810.1.1 POLICY STATEMENT

(1) The drug collection and disposal program provides a safe disposal location for citizens to properly dispose of unused prescription medications.

(a) This program provides an environmentally safe alternative to disposing of medications in the landfill or sewer systems which may later negatively effect the environment.

(b) This program encourages citizens to remove their unneeded medications from their homes. This reduces access to addictive medications for accidental or intentional misuse by children in the home.

(2) South Salt Lake Police Department will provide steel mailbox style collection boxes in which citizens may deposit these medications.

(a) Collection boxes shall be clearly marked for this purpose

(b) Collection boxes shall be locked to prohibit removal of the box or retrieval of medications from within the box without a key.

(c) Citizens may place their unused medications/drugs into the collection box anonymously.

(d) Medications can be placed into the drug collection drop box in their original prescription bottle/ packaging.

(e) Syringes should not be placed in the drop box.

(e) Opened containers of liquid will not be accepted unless they are completely sealed.

810.1.2 PROCEDURES

(3) The Investigations Commander will be responsible for collection of the deposited medications.

(a) The Investigations Commander or an evidence technician will be the sole possessors of keys to the collection boxes.

(i) Police Department Personnel shall not have access to the contents of the collection boxes.

(ii) Police Department Personnel may monitor the collection of the drop box contents with Evidence Staff. This allows officers the ability to survey the kinds of drugs and medications that are being disposed of. This information can be used for evaluation and decisions regarding the program.

(b) A case number will be assigned to each removal of drugs from the collection box. The Investigations Commander or designee will document each collection in the designated records management system This allows for tracking of data to monitor the programs benefits.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Pharmaceutical Drug Collection Program

(c) The Investigations Commander or designee and an additional SSLPD employee will collect the deposited drugs on a frequency deemed necessary based on the location and usage.

(d) The Investigations Commander or designee and an additional SSLPD employee will bag the deposited drugs, document a general description of the contents, provide a weight of the contents, and place into evidence pending destruction.

(e) The Evidence Unit will destroy the collected medications by incineration through a contracted provider of this service.

(f) The Investigations Commander will provide a monthly reporting of the pounds of Medications collected to the Utah Department of Environmental Quality via email at:

llamb@utah.gov

Victim Advocates

811.1 PURPOSE AND SCOPE

The purpose of this policy is to outline responsibilities and roles for the victim advocates.

811.2 POLICY

It is the policy of the South Salt Lake Police Department Victim Advocate Program to comply with State and Federal laws, grant requirements, and mandates for programmatic procedures.

811.3 ABBREVIATIONS

BT - Bench Trial

JT- Jury Trial

ADC - Adult Detention Center, means that DEF is attending Webex court from jail

PIA - Plea in Abeyance, means conviction is in a state of temporary suspension (typically 12 months)

PO - Protective Order

CSI - Civil Stalking Injunction

PTPO - Pretrial PO

SNTPO - Sentencing PO

ARR - Arraignment

PTC- Pretrial Conference

VIS- Victim Impact Statement

DC- District Court

DAO- District Attorney's Office

SGI- Notice of Safeguarded Info, this is what we send to prosecution/court clerks when a victim is requesting a protective order.

NCO- No contact order

SUDS- Substance Abuse Disorder (a treatment option in court)

LA - Legal Aid

PARC- Pamela Atkinson Resource Center, also referred to as MRC (Men's Resource Center) this is the men's only homeless shelter in our area.

CM- case manager

VTs- Victim Tracking Services

CVR- Crime Victim Reparations

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Victim Advocates

UOVC- Utah Office for Victims of Crime

IPV- Interpersonal Violence

CSI- Civil Stalking Injunction

LAP- Lethality Assessment Protocol

811.4 VICTIM SERVICES SUPERVISOR RESPONSIBILITIES AND CHECKLIST

A. Federal Grant Responsibilities

VOCA Federal Grant (supplements personnel of (3) victim advocates).

Quarterly federal progress reports and payment requests: April, July, October, and January

Quarterly PMT Report: April, July, October, January - Performance Measurement for Office of Justice Programs

Yearly SAR report as summary for quarterly PMT reports

VAWA Federal Grant (supplements personnel of two detectives (DV, sex assault))

Quarterly federal progress report and payment request: April, July, October, and January

Yearly Subgrantee Progress Report for U.S. Department of Justice

Annual Federal Grant Desk Audits (VOCA/VAWA)

To assess progress towards stated project goals, review previously submitted reports, and determine / confirm programmatic, financial, and administrative compliance.

B. South Salt Lake Justice Court

Completion of court notes (VA case status) and hearing schedules

Monitor court hearing schedule for applicable victim services cases

Upcoming hearings and the victim advocate case status notes entered in EXCEL document.

Weekly case notes are emailed to city prosecutors for entry into Eprosecutor

Protective order requests are submitted, and SGI information is sent to the court

C. Lethality Assessment Protocol (LAP)

Relay statewide and agency Lethality Assessment updates to all relevant personnel.

Ensure officers complete LAP in UCJIS and submit timely.

Receive and review completed LAPs (from UCJIS).

Upload all LAPs to victim's case file.

Forward Hi-Risk LAPs to: DV Detectives, and SVU Sergeant

Forward LAPs to court upon request.

Maintain strict confidentiality (VA team and supervisor responsibility).

D. UVISA Applications (USCIS I-918)

Manage incoming I-918 forms (from victims or attorneys).

Review for:

Applicable crime

Victim cooperation

Complete form and submit to:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Victim Advocates

Chief or Deputy Chief

Return original signed form to victim/attorney.

Ensure response is within 10 days of receipt.

E. Memorandums of Understanding (MOUs) – updated each 2-year grant cycle

Rape Recovery Center

Coordinate with Laura Byl (Mobile Response Team Director)

Maintain agreement to: Coordinate with mobile response team on Code R exams

Collaborate using SART protocol

Ensure seamless service delivery and ongoing care for survivors

Quarterly collaboration meetings to discuss standards of care and resolve issues

F. File MOU in Documents/LAP/LAP MOU – signed SOSLPD

Wasatch Forensic Nurses (WFN) Coordinate with Trish Crump (Law Enforcement Liaison)

Contact WFN through answering service for IPV and Code R forensic exams

Keep current on IPV exam funding status and disseminate to detectives and advocates.

G. Quarterly collaboration meetings to discuss standards of care and resolve issues South Salt Lake Justice Court

Weekly exchange of applicable case information for upcoming hearings

Timely submission of protective order requests and completed SGI information

Coordinate direct contact between victims and prosecutors as needed

Quarterly collaboration meetings to discuss standards of care and resolve issues

H. Scheduling / Coverage / Hearings

Create Monthly On-Call Schedule

Include 3 VAs on weekly rotation

Email by 1st of month to: Command Staff and VECC Dispatch (Elyse Haggerty) Communicate any changes to dispatch.

I. Maintain Justice Court Coverage:

Coordinate with city prosecutors and court staff

Assign advocates to daily hearings (in-person/Webex)

Update Google Sheet: Justice Court Cases

Email weekly case notes to prosecutors

Ensure paralegal uploads case notes to Eprosecutor

J. Purchasing Responsibilities

Emergency Funds

Maintain \$500 petty cash

Access shared with Investigations Lieutenant

Use funds for: Food, hygiene items, Childcare needs, One-night hotel (immediate shelter/safety plan)

Track purchases in Excel and provide receipts to Police Executive Assistant for reimbursement

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Victim Advocates

Victim Services Tracking System Yearly Billing

Monitor end-of-year invoice from Online Web Services. Due by December 14

Forward invoice to the Police Executive Assistant for HR payment processing.

K. Meetings and Training

Attend Wellness Committee (monthly, City Hall)

Attend Command Staff Meeting (monthly)

Attend Rape Recovery/Wasatch Forensic Collaboration Meeting (monthly, Zoom)

Attend Justice Court/City Prosecutors Meetings (as needed and quarterly)

Conduct Victim Services Team Meeting (biweekly)

Participate in SART training (monthly, Zoom)

Participation in DPS/SBI Training (monthly, Zoom)

Present to City Council (Federal Grant Report) (biannually)

Join VOCA/VAWA UOVC Technical Assistance (quarterly, Google Meet)

811.5 VICTIM SERVICES ADVOCATE RESPONSIBILITIES

General Call-Out Procedures

- Prioritize the **victim's (VIC) safety** and create a safety plan.
- Discuss **protective orders (PO)** and other resources like **Crime Victim Reparations (CVR)**, explaining that more details can be provided later.

Sex Assault Call-Out Procedures

- Obtain VIC name, phone number, case number, and a brief crime description.
- Ask if the VIC wants a **Forensic Exam**.
 - If yes, ask for their preferred hospital.
 - Call **Wasatch Forensic Nurses (WFN)** at (801) 461-5888; provide VIC's full name, birthdate, and case number.
- Offer transportation to the hospital for support.
- Explain that **Rape Recovery** will also provide support.
- Complete a **Medical Release Form** on behalf of assigned detective

Domestic Violence Call-Out Procedures

- Obtain VIC name, phone number, case number, and a brief crime description.
- If **defendant (DEF)** was arrested, explain **Jail Release Agreement (JRA)**. If not, address in safety planning.
- For **High-Risk LAP's**, inform VIC about **YWCA's 72-hour room** and ensure officers contact YWCA to speak with VIC.
- Provide local shelter information:
 - YWCA: (801) 537-8600

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Victim Advocates

- SVS: (801) 255-1095
- Farther shelters: Safe Harbor Crisis Center (Layton) (801) 444-9161, The Refuge (Orem) (801) 227-5038, YCC (Ogden) (801) 394-9456.
- Check for funding availability for a hotel/motel stay.

On-Call Week Caseload & Follow-Up

Any case during your on-call week is part of your caseload.

- Cases are assigned by victim services supervisor and placed in VA queue.
- **Follow up with victims within 3 business days.**
- If no contact, try all options (email, letter).
- For homeless male victims, add to **PARC Spreadsheet** for case manager contact.
- Monitor your assigned cases on the **Monitoring List**.
- No follow-up needed for DV verbals unless necessary (e.g., multiple incidents with VIC).

Initial Follow-Up

- Ask about **safety, well-being, and immediate needs** (shelter, PO, etc.).
- Explain your role (investigation, court, resources).
- Try to get an email address.
- **If still under investigation:** Explain a **detective (DET)** will be/has been assigned; facilitate communication.
- **If arrest/citation given or DET sent for screening:** Explain case sent to court (Justice or District) and offer updates.

Court-Related Questions

- Ask if the victim wants a **Pretrial Protective Order (PTPO)**.
- Ask about opinions on charges (e.g., plea in abeyance, beneficial treatment).
- Ask if the victim wants to participate in court (in person or WebEx).
- Ask if the victim wants to complete a **Victim Impact Statement (VIS)**.
- Explain **CVR** and ask about interest; offer to email the form or fill it out in person.

Court Updates & Contacts

General:

- Check **Xchange** for all court updates (ensure correct jurisdiction and case number).
- Search by name on Xchange if no case number; use an asterisk for partial names (e.g., Smith*).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Victim Advocates

Justice Court:

- Use the **Utah Court Calendar** for case info, add to the **Justice Court Calendar** with case notes.
- Ensure notes are completed by Friday morning for prosecutor email
- Check **Screening Log** for cases being screened

District Court

- Use **Eprosecutor** to check cases being screened.
- Find **District Attorney Victim Advocate (DA VA)**, attorney, legal secretary, and paralegal here.
- Not all DC cases have a victim advocate; be prepared to continue assisting VIC or refer to Victim Support Services Division.
- For declined cases refer to DA's MDT Legal Secretary

Protective Orders (PO)

Pretrial Protective Orders (PTPO)

- **Justice Court PTPO:**
 - Complete **Notice of Safeguarded Info (SGI)**.
 - Send to Mayra Serna, Rebecca Stone, Natalie Molino, and cc assigned attorney.
 - Include the relationship between parties and PO specifications (e.g., child communication, third-party contact) in email.
 - Add SGI to documents on **Victim Tracking Services (VTS)**.
- **District Court PTPO:**
 - Commonly issued at Initial Appearance (IA) or first scheduling conference for DV/SA cases.
 - Contact DA VA or Attorney to confirm PO placement or specifications.

Post-Court PO Options

- **Sentencing PO:** Lasts for probation duration.
- **Continuous PO:** Lasts indefinitely unless VIC requests a hearing to rescind.

Alternative PO Options (if VIC doesn't want to wait for court)

- **Legal Aid:** Best option.
 - Can complete the intake over the phone.
 - Legal Aid will contact VIC within 15-30 minutes during office hours.
 - Temporary PO usually within 1-2 days if represented.
 - Court hearing at DC for permanent PO.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Victim Advocates

- **If declined by Legal Aid:**
 - **Online Court Assistance Program (OCAP):** Pro se application.
 - **Utah Crime Victims Legal Clinic (UCVLC):** May represent VIC.
 - Hire a private attorney (financial costs apply).
- Do not assist with **restraining orders** (victim needs their own attorney).
- **Civil Stalking Injunctions** can be applied for via Legal Aid or other listed options; requires at least two police reports/instances.

Jail Release Agreements (JRA)

- Victims can waive JRA; assist if they are aware of this right.
- If DEF is in custody, VIC can fill out waiver at your location.
- Detective, sergeant, or any officer can sign the waiver.
- Send signed waiver to

Jail Court Liaison: (385) 468-8461 or adc-court1@slco.org.

- If DEF is not in custody, the court must address this (VIC can call JC/DC for PO hearing or earlier arraignment).
- JRA expires in 30 days or at midnight on the day of arraignment (whichever comes first).

Crime Victim Reparations (CVR)

- For victims with physical/psychological injury or death due to criminal conduct.
- Victims not cooperating with law enforcement/courts likely won't qualify.
- Screening takes about a month; tell victims to keep bills.
- May pay up to \$2000 in relocation funds if qualified.
- **CVR Application:** VIC fills sections 1, 3, 8, 9; you fill sections 4, 5, 7.
- Attach completed application to case documents in VTS.

Victim Tracking Services (VTS)

- First case note: brief crime description, starting with "Per LE report".
- Make a case note each time you speak with or assist a victim.
- Keep notes concise, objective.
- **Highlight important information in yellow** (e.g., PO request, court participation interest).

Miscellaneous Resources

- Emergency Phones

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Victim Advocates

- Promise Resource Guide
- Mental Health Providers
- Stalking Log
- DV Lease Termination
- DV Support Group.
- **VINELink:** Victims can check DEF custody status.
- **Interpreter Services:**
 - **Linguistica:** (801) 262-4550 (Department # 01219).
 - **Interwest Interpreting (ASL):** (866) 224-7683 (requires appointment).

CJIS Access, Maintenance, and Security

813.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the use, maintenance, and security of [department/office] systems that access Criminal Justice Information.

813.1.1 DEFINITIONS

Definitions related to this policy include:

Criminal Justice Information (CJI) - Data provided by FBI Criminal Justice Information Services (CJIS) that is necessary for law enforcement agencies to perform their mission and enforce the laws (e.g., biometric, identity history, person, organization, case/incident history data).

Security incident - Any incident that compromises the security of CJI or systems that access CJI. Examples include but are not limited to unauthorized use of legitimate code or credentials within [department/office] systems, email communications that contain malicious code, data breaches, signaling to external systems, and unauthorized exporting of information.

813.2 POLICY

It is the policy of the South Salt Lake Police Department to maintain the security, confidentiality, and integrity of its information systems that access CJI by collaborating with appropriate state and federal agencies to implement the applicable established protocols.

813.3 CJIS COORDINATOR

The Chief of Police shall appoint a CJIS coordinator, who shall be responsible for the South Salt Lake Police Department's adherence to FBI CJIS Security Policy requirements.

The CJIS coordinator shall establish procedures necessary to govern the [department/office]'s use, maintenance, and security of systems that access CJI as described in this policy.

813.3.1 CJIS COORDINATOR RESPONSIBILITIES

The responsibilities of the CJIS coordinator include but are not limited to:

- (a) Coordinating with others, such as the information technology or legal departments, as appropriate, to maintain [department/office] compliance with FBI CJIS Security Policy requirements and the Utah Bureau of Criminal Identification (BCI).
- (b) Managing member accounts with access to CJI, including:
 - 1. Creating, enabling, modifying, disabling, and removing member accounts in accordance with this policy and the FBI CJIS Security Policy.
 - 2. Configuring member accounts in accordance with federal and state requirements (e.g., limiting unsuccessful login attempts).
 - 3. Reviewing member accounts for compliance with legal and policy requirements at least annually.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

CJIS Access, Maintenance, and Security

- (c) Overseeing the maintenance, repair, and replacement of CJI systems and system components in accordance with manufacturer or vendor specifications and/or [department/office] requirements, including:
 - 1. Maintaining a list of organizations and personnel approved by the Chief of Police to perform maintenance on CJI systems.
 - 2. Approving, scheduling, documenting, and monitoring all maintenance and diagnostic activities, whether performed on-site, remotely, or off-site, and maintaining records.
 - 3. Verifying that non-escorted personnel performing maintenance on any CJI system or terminal possess the required access authorizations, and designating members who have the required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
 - 4. Maintaining records for all system maintenance and diagnostic activities.
- (d) Monitoring [department/office] systems that have access to CJI to ensure compliance with applicable laws and this policy; developing processes to detect, identify, and correct flaws in software and firmware; and conducting security updates as necessary.
- (e) Providing for the security of hardware that includes provisions for the following:
 - 1. How hardware is to be brought into and taken out of [department/office] facilities
 - 2. Physical security of hardware within [department/office] facilities
 - 3. Physical security of areas containing network connections and transmission lines, including monitored access
- (f) Implementing and carrying out the [department/office] Incident Response Plan, including:
 - 1. Tracking and documenting all suspected or actual security incidents related to CJI in an appropriate manner.
 - 2. Directing annual testing of the [department/office]'s information security incident response capabilities using tabletop or walk-through exercises, simulations, or other types of testing.
 - 3. Making the appropriate notifications outside of the [Department/Office] (see the Records Maintenance and Release Policy for additional guidance).
 - 4. Providing information on security incidents to any third-party software developers or vendors as appropriate.
- (g) Protecting digital and non-digital media that contain CJI, including physical security, transportation, destruction/sanitization, and documentation requirements.
- (h) Developing and updating [department/office] information security and privacy literacy training and incident response training as required by policy.
- (i) Maintaining audit records in accordance with the established records retention schedule, but in no event for less than one year.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

CJIS Access, Maintenance, and Security

- (j) Managing the development, documentation, and dissemination of procedures for the following:
 - 1. Awareness and training
 - 2. Incident response
 - 3. Audit and accountability
 - 4. Access control
 - 5. Identification and authentication
 - 6. Configuration management
 - 7. Media protection
 - 8. Physical and environmental protection
 - 9. System and communications protection
 - 10. System and information integrity
 - 11. Maintenance
 - 12. Security and privacy planning
 - 13. Contingency planning
 - 14. Risk assessment
- (k) Reviewing this policy and related procedures as required by the FBI CJIS Security Policy and proposing updates as needed to the Chief of Police.

813.4 MEMBER RESPONSIBILITIES

All members of the [Department/Office] shall be committed to detecting information security incidents and making the appropriate notifications.

Any member who suspects that there may have been unauthorized access, disclosure, or other compromise of CJI shall report their suspicions in accordance with the Incident Response Plan within one hour of the discovery.

Personally owned devices or systems and publicly accessible systems shall not be used to access, process, store, or transmit CJI.

813.5 SUPERVISOR RESPONSIBILITIES

Supervisors shall notify the CJIS coordinator when the account access of a member they supervise needs to be modified, disabled, or removed for any reason, such as resignation, termination, or change of duties.

813.6 MEMBER ACCOUNTS

[Department/Office] accounts used to access CJI shall only be created upon approval of the Chief of Police or the authorized designee.

Member accounts shall be disabled within one week of any of the following:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

CJIS Access, Maintenance, and Security

- (a) The account has expired.
- (b) The account is no longer associated with a member.
- (c) The account is found to be in violation of this policy.
- (d) The account has been inactive for 90 calendar days.

If any threat to the confidentiality, integrity, or availability of CJI related to a specific member account is detected, the CJIS coordinator or designated member shall disable the account within 30 minutes of the discovery.

813.6.1 ACCESS AUTHORIZATION

Access authorization for systems transmitting, receiving, using, or storing CJI shall be based on the principle of least privilege as follows:

- (a) Members shall only be granted access authorizations that are necessary to accomplish assigned [department/office] tasks.
- (b) Accounts with security privileges shall only be authorized for members with an operational need for the privileges. Privileged functions shall be logged as they are executed.
- (c) Non-privileged members shall not be allowed to execute privileged functions.

813.6.2 ACCOUNT REVIEW ACTIVITIES

At least annually, the CJIS coordinator shall review member accounts for compliance with policy and applicable laws. The CJIS coordinator shall validate account privileges and remove or reassign them as necessary to accurately reflect the [department/office] mission and law enforcement needs.

813.7 MEDIA PROTECTION

Access to media containing CJI shall be restricted to authorized members and stored within physically secured locations or controlled areas, in accordance with the FBI CJIS Security Policy.

Digital media (e.g., flash drives, external or removable hard disk drives, compact discs) containing CJI shall be encrypted. Personally owned digital media devices or digital media devices with no identifiable owner shall not be used on [department/office] systems that store, process, or transmit CJI.

Non-digital media (e.g., paper files, printed pages, microfilm) containing CJI should be enclosed in an opaque folder or container if they are to be transported outside of physically secure locations or controlled areas. Media containing CJI shall not be left unattended outside of a physically secure location.

Transportation and transfers of media containing CJI shall be documented.

813.7.1 MEDIA DISPOSAL AND RELEASE

Digital media containing CJI shall be overwritten at least three times or degaussed (i.e., erased) prior to being disposed of, released from [department/office] control, or released for reuse.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

CJIS Access, Maintenance, and Security

Inoperable digital media devices, such as hard drives or solid-state drives that cannot be accessed to overwrite the data, shall be physically destroyed. When non-digital media is no longer needed for investigative or security purposes, it shall be destroyed by crosscut shredding or incineration.

813.8 SYSTEM AND INFORMATION INTEGRITY

The integrity of [department/office] CJI systems shall be protected through the implementation of appropriate controls such as:

- (a) Flaw remediation.
- (b) System monitoring.
- (c) Security alerts, advisories, and directives.
- (d) Software, firmware, and information integrity controls.
- (e) Spam protection.

813.9 INCIDENT RESPONSE PLAN

Contact the Deputy Chief and IT.

813.10 SECURITY AWARENESS TRAINING

Members with physical or electronic access to CJI or CJI systems shall complete security awareness training appropriate to their assigned roles and responsibilities and shall certify their understanding by signing a formal Security Awareness Training Acknowledgement. Training shall include information security and privacy literacy training, security incident response training, and a review of this policy and related procedures.

Security awareness training shall be completed prior to accessing any CJI data or system and at least annually thereafter. Additional training shall be completed as required following any changes to CJI systems and for any member involved in a security incident within 30 days of the event.

Individual training records shall be maintained in accordance with the established records retention schedule, but in no event for less than three years.

The [department/office]'s CJIS training shall be reviewed for any necessary updates or changes annually and following any security incident or change in a CJI system or the FBI CJIS Security Policy.

813.11 SANCTIONS

Failure to adhere to policies and procedures pertaining to CJI shall result in disciplinary action, up to and including termination. Misuse of or failure to secure CJI may also result in temporary or permanent restrictions in the use of CJI. Intentional misuse of CJI may also be prosecutable under applicable laws.

Chapter 9 - Custody

Temporary Custody of Adults

900.1 PURPOSE AND SCOPE

This policy provides guidelines to address the health and safety of adults taken into temporary custody by members of the South Salt Lake Police Department for processing prior to being released or transferred to a housing or other type of facility.

Temporary custody of juveniles is addressed in the Temporary Custody of Juveniles Policy. Juveniles will not be permitted where adults in custody are being held.

Custodial searches are addressed in the Custodial Searches Policy.

Additional guidance for transferring persons in custody to another facility or court is provided in the Transporting Persons in Custody Policy.

900.1.1 DEFINITIONS

Definitions related to this policy include:

Holding cell/cell - Any locked enclosure for the custody of an adult or any other enclosure that prevents the occupants from being directly visually monitored at all times by a member of the Department.

Safety checks - Direct, visual observation by a member of this department performed at random intervals, within time frames prescribed in this policy, to provide for the health and welfare of adults in temporary custody.

Temporary custody - The time period an adult is in custody at the South Salt Lake Police Department prior to being released or transported to a housing or other type of facility.

900.2 GENERAL CRITERIA AND SUPERVISION

No adult should be in temporary custody for longer than six hours.

900.2.1 SUPERVISION IN TEMPORARY CUSTODY

An authorized department member capable of supervising shall be present at all times when an individual is held in temporary custody. The member responsible for supervising should not have other duties that could unreasonably conflict with his/her supervision. Any individual in custody must be able to summon the supervising member if needed. If the person in custody is deaf or hard of hearing or cannot speak, accommodations shall be made to provide this ability.

At least one female department member should be present when a female adult is in temporary custody. In the event that none is readily available, the female in custody should be transported to another facility or released pursuant to another lawful process.

Absent exigent circumstances, such as a medical emergency or a violent subject, members should not enter the cell of a person of the opposite sex unless a member of the same sex as the person in custody is present.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Custody of Adults

No individual in custody shall be permitted to supervise, control or exert any authority over other individuals in custody.

900.2.2 ENTRY RESTRICTIONS

Entry into any location where a person is held in custody should be restricted to:

- (a) Authorized members entering for official business purposes.
- (b) Emergency medical personnel when necessary.
- (c) Any other person authorized by the Watch Commander.

When practicable, more than one authorized member should be present for entry into a location where a person is held in custody for security purposes and to witness interactions.

900.3 INITIATING TEMPORARY CUSTODY

The officer responsible for an individual in temporary custody should evaluate the person for any apparent chronic illness, disability, vermin infestation, possible communicable disease or any other potential risk to the health or safety of the individual or others. The officer should specifically ask if the individual is contemplating suicide and evaluate him/her for obvious signs or indications of suicidal intent.

The receiving officer should ask the arresting officer if there is any statement, indication or evidence surrounding the individual's arrest and transportation that would reasonably indicate the individual is at risk for suicide or critical medical care. If there is any suspicion that the individual may be suicidal, he/she shall be transported to the City jail or the appropriate mental health facility.

The officer should promptly notify the Watch Commander of any conditions that may warrant immediate medical attention or other appropriate action. The Watch Commander shall determine whether the individual will be placed in a cell, immediately released or transported to jail or other facility.

900.3.1 SCREENING AND PLACEMENT

The officer responsible for an individual in custody shall:

- (a) Advise the Watch Commander of any significant risks presented by the individual (e.g., suicide risk, health risk, violence).
- (b) Evaluate the following issues against the stated risks in (a) to determine the need for placing the individual in a single cell:
 - 1. Consider whether the individual may be at a high risk of being sexually abused based on all available known information (28 CFR 115.141), or whether the person is facing any other identified risk.
 - 2. Provide any individual identified as being at a high risk for sexual or other victimization with heightened protection. This may include (28 CFR 115.113; 28 CFR 115.141):
 - (a) Continuous, direct sight and sound supervision.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Custody of Adults

- (b) Single-cell placement in a cell that is actively monitored on video by a member who is available to immediately intervene.
- 3. Ensure individuals are separated according to severity of the crime (e.g., felony or misdemeanor).
- 4. Ensure individuals are separated based upon their sex, as defined by Utah Code 68-3-12.5, by sight and sound when in cells (Utah Code 63G-31-201).
- 5. Ensure restrained individuals are not placed in cells with unrestrained individuals.
- (c) Ensure that those confined under civil process or for civil causes are kept separate from those who are in temporary custody pending criminal charges.
- (d) Ensure separation, as appropriate, based on other factors, such as age, criminal sophistication, assaultive/non-assaultive behavior, mental state, disabilities, and sexual orientation.

900.3.2 CONSULAR NOTIFICATION

Consular notification may be mandatory when certain foreign nationals are arrested. The Patrol Division Commander will ensure that the U.S. Department of State's list of countries and jurisdictions that require mandatory notification is readily available to department members. There should also be a published list of foreign embassy and consulate telephone and fax numbers, as well as standardized notification forms that can be transmitted and then retained for documentation. Prominently displayed signs informing foreign nationals of their rights related to consular notification should also be posted in areas used for the temporary custody of adults.

Department members assigned to process a foreign national shall:

- (a) Inform the individual, without delay, that he/she may have his/her consular officers notified of the arrest or detention and may communicate with them.
 - 1. This notification should be documented.
- (b) Determine whether the foreign national's country is on the U.S. Department of State's mandatory notification list.
 - 1. If the country is on the mandatory notification list, then:
 - (a) Notify the country's nearest embassy or consulate of the arrest or detention by fax or telephone.
 - (b) Tell the individual that this notification has been made and inform him/her without delay that he/she may communicate with consular officers.
 - (c) Forward any communication from the individual to his/her consular officers without delay.
 - (d) Document all notifications to the embassy or consulate and retain the faxed notification and any fax confirmation for the individual's file.
 - 2. If the country is not on the mandatory notification list and the individual requests that his/her consular officers be notified, then:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Custody of Adults

- (a) Notify the country's nearest embassy or consulate of the arrest or detention by fax or telephone.
- (b) Forward any communication from the individual to his/her consular officers without delay.

900.4 HOLDING CELLS

A thorough inspection of a cell shall be conducted before placing an individual into the cell to ensure there are no weapons or contraband and that the cell is clean and sanitary. An inspection also should be conducted when the individual is released. Any damage noted to the cell should be photographed and documented.

The following requirements shall apply:

- (a) The individual shall be searched (see the Custodial Searches Policy), and anything that could create a security or suicide risk, such as contraband, hazardous items, belts, shoes or shoelaces, and jackets, shall be removed.
- (b) The individual shall constantly be monitored by an audio/video system during the entire custody.
 - 1. Audio/video equipment shall be controlled to reduce any unnecessary invasion of the individual's personal privacy.
- (c) The individual shall have constant auditory access to [department/office] members.
 - 1. An audio system that enables the individual to alert a dispatcher or an officer in the event of emergency shall remain on at all times when an individual is in a cell.
 - 2. In the event the audio system is inoperative or non-operational, a member shall be assigned to monitor the individual.
- (d) The individual's initial placement into and removal from a locked enclosure shall be logged.
- (e) Safety checks by [department/office] members shall occur no less than every 15 minutes.
 - (a) Safety checks should be at varying times.
 - (b) All safety checks shall be logged.
 - (c) The safety check should involve questioning the individual as to their well-being.
 - (d) Individuals who are sleeping or apparently sleeping should be awakened.
 - (e) Requests or concerns of the individual should be logged.
 - (f) Access to water, restrooms and other needs shall be accommodated.
- (f) Clean blankets are provided as reasonably necessary to ensure the comfort of an individual.
 - 1. The supervisor should ensure that there is an adequate supply of clean blankets.
- (g) A documented face-to-face count of the detainee population shall be conducted at least once every eight hours.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Custody of Adults

900.4.1 RECEIVING ITEMS

Individuals in temporary custody shall not receive personal items, mail, or packages while being detained in a cell.

900.4.2 CELL EQUIPMENT CONTROL

Culinary devices (e.g., utensils, plates, glassware) should not be permitted in cells where individuals are in custody. Meals, if provided, should be consumable without culinary devices.

If repairs are necessary to any part of the cell area:

- (a) Individuals in temporary custody shall not be present in the immediate area of such work.
- (b) Maintenance employees or contract workers shall not enter the cell area without authorization from a supervisor.
- (c) A member shall monitor the use of any tools and equipment in the area for the duration of the work.
- (d) The supervising member shall ensure that workers have removed all tools and equipment and conduct a documented security inspection of the cell area upon completion of the work.

900.4.3 VISITORS

Visitation of individuals in temporary custody should not be permitted.

The Watch Commander may authorize an attorney to visit with an individual in temporary custody for the purpose of private consultation, subject to the following:

- (a) The visiting attorney's name and address shall be recorded.
- (b) The visiting attorney and any belongings should be searched before the visit.
- (c) Visits should take place in an authorized interview room or temporary detention area.
 - 1. The visitation shall be monitored from outside the room or area, and audio recording equipment shall be turned off during the visit.

900.4.4 EXCEEDING CAPACITY

In the event of a mass arrest, individuals should be placed in an appropriate holding cell, handcuffed to a fixed object approved for such use, kept secure in a transport vehicle, or otherwise secured as directed by the Watch Commander. Areas used for temporary custody under these circumstances shall be inspected for weapons, objects that may be used as weapons, and contraband before and after use.

Temporary overcrowding of a holding cell is permitted under these circumstances until such time as the overcrowding situation can be reasonably relieved, through the transfer or release of persons being held. An officer shall be assigned to a cell area for the purpose of maintaining security whenever there is an overcrowding situation.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Custody of Adults

If releasing a sufficient number of detainees to relieve the temporary overcrowding situation is not practicable, the Watch Commander shall request the use of neighboring law enforcement agencies' holding facilities with the use of [department/office] members to maintain security and control, if requested by the other agency.

900.5 SUICIDE ATTEMPT, DEATH OR SERIOUS INJURY

The Patrol Division Commander will ensure procedures are in place to address any suicide attempt, death or serious injury of any individual in temporary custody at the South Salt Lake Police Department. The procedures should include the following:

- (a) Immediate request for emergency medical assistance if appropriate.
- (b) Immediate notification of the Watch Commander, Chief of Police and Investigation Division Commander.
- (c) Notification of the spouse, next of kin or other appropriate person.
- (d) Notification of the appropriate prosecutor.
- (e) Notification of the City Attorney.
- (f) Notification of the Medical Examiner.
- (g) Evidence preservation.

900.6 MEDICAL CARE AND IN-CUSTODY SUSPECTS AT MEDICAL FACILITIES

First-aid equipment and basic medical supplies should be available to department members. At least one member who has current certification in basic first aid and CPR should be on-duty at all times.

Should a person in custody be injured or become ill, appropriate medical assistance should be sought. A supervisor should meet with those providing medical aid at the facility to allow access to the person. Members shall comply with the opinion of medical personnel as to whether an individual in temporary custody should be transported to the hospital. If the person is transported while still in custody, they will be accompanied by an officer.

Those who require medication while in temporary custody should not be held at the South Salt Lake Police Department. They should be released or transferred to another facility as appropriate.

900.7 RELEASE AND/OR TRANSFER

When an individual is released or transferred from custody, the member releasing the individual should ensure the following:

- (a) All proper reports, forms, and logs have been completed prior to release.
- (b) A check has been made to ensure that the individual is not reported as missing and does not have outstanding warrants.
- (c) It has been confirmed that the correct individual is being released or transported.
- (d) All property, except evidence, contraband, or dangerous weapons, has been returned to, or sent with, the individual.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Custody of Adults

- (e) All pertinent documentation accompanies the individual being transported to another facility (e.g., copies of booking forms, medical records, an itemized list of property, warrant copies).
- (f) The individual is not permitted in any nonpublic areas of the South Salt Lake Police Department unless escorted by a member of the [Department/Office].
- (g) Any known threat or danger the individual may pose (e.g., escape risk, suicide potential, medical condition) is documented, and the documentation transported with the individual if the individual is being sent to another facility.
- (h) Transfers between facilities or other entities, such as a hospital, should be accomplished with a custodial escort of the same sex as the person being transferred to assist with the person's personal needs as reasonable.

900.8 ASSIGNED ADMINISTRATOR

The Patrol Division Commander will ensure any reasonably necessary supplemental procedures are in place to address the following issues:

- (a) General security
- (b) Key control
- (c) Sanitation and maintenance
- (d) Emergency medical treatment
 - 1. A first aid kit shall be available in all facilities.
 - 2. First aid kits shall be inspected periodically and replenished when necessary.
- (e) Escapes
- (f) Evacuation plans
 - 1. The facility shall have a written and posted emergency evacuation plan and designated and signed emergency exit(s) directing evacuation of persons to hazard-free areas.
- (g) Fire- and life-safety
 - 1. Temporary detention areas and cells shall have an automatic fire alarm and heat and smoke detection system, and fire equipment approved in writing by state or local fire officials.
 - 2. Fire equipment (i.e., extinguishers) and fire detection devices shall be inspected and tested as required by applicable fire codes.
- (h) Disaster plans
- (i) Building and safety code compliance

900.9 TRAINING

Department members should be trained and familiar with this policy and any supplemental procedures.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Custody of Adults

900.9.1 ADDITIONAL TRAINING REQUIREMENTS

[Department/Office] members shall be trained in the operations of the holding facility, including fire suppression and equipment provided for use by the [Department/Office].

900.10 RECEIVING DETAINEES FROM AN OUTSIDE AGENCY

If a member of an outside agency presents an individual to be held in temporary custody at the [Department/Office], the person presenting the individual shall be positively identified. If unknown, the person presenting the individual in custody should be required to produce appropriate identification and their legal authority to make the commitment.

Arrest With or Without a Warrant

901.1 PURPOSE AND SCOPE

The purpose of this policy is to define the authority of officers to arrest, and the mechanism for making arrests with and without a warrant. Arrests are very serious police actions. Officers shall accordingly exercise critical judgment in making arrests. Officers shall also consider alternatives to arrest consistent with their law enforcement mission. This policy recognizes that occasionally circumstances exist, such as jail capacity, that would preclude the officer from effecting an arrest when otherwise appropriate.

901.2 DEFINITIONS

- (a) **Arrest** - An actual restraint of the person arrested or submission to custody. The person shall not be subjected to any more restraint than is necessary for the person's arrest and detention. Officer safety must be considered if the arrested person(s) remain violent after arrest.
- (b) **Reasonable Suspicion** - Facts and circumstances which, taken together with reasonable inferences in light of an officer's training and experience and measures in terms of common sense, would cause an officer to suspect that:
 - 1. A person has been, is, or is about to be, involved in criminal activity (Stop).
 - 2. A person is armed with a quickly accessible weapon and constitutes a danger to the officer (Frisk).
- (c) **Search** - A police action that infringes upon a person's reasonable expectation of privacy.

901.3 AUTHORITY TO ARREST

- (a) Statute for Daytime/Nighttime No-knock:
 - 1. A felony arrest warrant may be served at any time of the day or night.
 - 2. A misdemeanor arrest warrant may be served at night only if:
 - (a) The magistrate has endorsed authorization to do so on the warrant.
 - (b) The person to be arrested is upon a public highway or in a public place open to or accessible to the public.
 - (c) The person is to be arrested is encountered by a peace officer in the regular course of that peace officers investigation of a criminal offense unrelated to the misdemeanor warrant for arrest. UCA 77-7-5.
- (b) Arrests with a Warrant:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Arrest With or Without a Warrant

- (a) Who: An arrest warrant may be issued by any magistrate or judge of any circuit court, district court, juvenile court, or justice court. UCA 77-7-5, 78-5-106(2), and URCr.P 6.
- (b) When to issue, what to recite: A magistrate or judge may issue a warrant for arrest upon finding probable cause to believe that the person to be arrested has committed a public offense. UCA 77-7-5(1).
- (c) What the warrant contains: If the magistrate determines that the accused must appear in court, the magistrate shall include in the arrest warrant the name of the law enforcement agency in the county municipality with jurisdiction over the offense charged. The warrant must not be too general or leave too much discretion to the officer to decide which suspect to arrest. UCA 77-7-5(2).
- (c) Serving a warrant:
 - (a) Service when not in possession of warrant - Any peace officer who has knowledge of an outstanding warrant of arrest may arrest a person he/she reasonably believes to be the person described in the warrant, without the peace officer having physical possession of the warrant. UCA 77-7-11.
 - (b) Warrant to show upon request - The officer need not have possession of the warrant at the time of arrest, but upon request shall show the warrant to the defendant as soon as practical. URCr.P 6(c)(3).
 - (c) Informing arrested person of charges - If the officer does not have possession of the warrant at the time of the arrest, the arrested person will be informed of the charges and the fact that a warrant exists. URCr.P 6(c)(3).
 - (d) A warrant shall be executed (the arrest of the accused) by a peace officer at any place within the State.
 - (e) A summons may be served by anyone authorized to serve a summons in a civil action. URCr.P 6(c)(3).
 - (f) Upon executing the warrant, the date of execution shall be noted on the warrant itself, and the warrant shall be returned to the magistrate as soon as practicable. URCr.P 6(c)(4).
- (d) Exemption of witnesses from arrest or service of process:
 - (a) If a person comes into this state in obedience to a summons directing him/her to attend and testify in this state he/she shall not, while in this state pursuant to such summons, be subject to arrest or the service of process, civil or criminal, in connection with matters which arose before his/her entrance into this state under the summons.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Arrest With or Without a Warrant

- (b) If a person passes through this state while going to another state in obedience to a summons to attend and testify in that state or while returning there from, he/she shall not while so passing through this state be subject to arrest or the service of process, civil or criminal, in connection with matters which arose before his/her entrance into this state under the summons. UCA 77-21-5, 78-24-12, 77-33-8.
- (e) Authority to Arrest Without a Warrant:
 - (a) The United States Constitution allows arrests to be made upon probable cause, without a warrant (except where a warrant is required to enter private premises). Utah law, however, requires that arrests be made pursuant to warrants except in certain specified circumstances.
 - (b) Officers have the power and authority, without process, to arrest and take into custody any person who shall commit or threaten to commit in the presence of the officer, or in the officer's view, any breach of the peace, or any offense directly prohibited by the laws of this State or by ordinance. UCA 10-3-915, 77-7-13, 77-7-2.
 - (c) Pursuant to 77-7-2 and 77-7-13, an officer may make a warrant-less arrest when:
 - (a) A person commits or attempts a crime in the officer's presence.
 - (a) "Presence" includes all of the physical senses or any device that enhances the acuity, sensitivity, or range of any physical sense, or records the observations of any of the physical senses.
 - (b) The officer has reasonable cause to believe a person has committed a felony, in or out of the officer's presence.
 - (c) The officer has reasonable cause to believe a person has committed a public offense, and there is reasonable cause to believe that the person may:
 - (a) Flee or conceal him/herself to avoid arrest.
 - (b) Destroy or conceal evidence of the commission of the offense.
 - (c) Injure another person or damage property belonging to another person.
 - (d) The officer has reasonable cause to arrest a person for shoplifting or library theft.
 - (e) The officer has reasonable information that the accused stands charged in the courts of a state with a crime punishable by death or imprisonment for a term exceeding one year. (Private citizen may also arrest under these conditions.)

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Arrest With or Without a Warrant

- (a) When so arrested, the accused must be taken before a judge or magistrate with all practicable speed and complaint must be made against him/her under oath, setting forth the grounds for the arrest and thereafter his/her answer shall be heard as if he/she had been arrested on a warrant. UCA 77-30-14.
- (f) The person is arrested based on a fugitive warrant from another state, see UCA 77-30-13. Any person who is found to be a fugitive from another state:
 - (a) Should be listed in a police report that will be active to investigations for further screening.
 - (b) Should be arrested based on the NCIC listing of the fugitive warrant and transported to a local detention facility until the screening and/or extradition process has been satisfied.
- (g) Officers may conduct warrant-less searches only in those areas within reach of the suspect for weapons and contraband unless otherwise directed by current case law.
- (h) Officers should advise every person of their constitutional rights, as directed by case law and prosecutorial direction.
 - (a) In most cases, this advisement should be done prior to the time a suspect is being questioned concerning the crime and when a suspect is in custody.
- (i) Regardless of the officer's knowledge of current case law, if any doubt exists as to whether a search warrant is needed or not, the officer should opt for a search warrant.
- (j) Officers should, after discussing the situation with their supervisor, utilize advice from the pertinent prosecutor's office whenever a question exists as to application of the laws of arrest, search and seizure, etc.

901.4 CITIZEN'S ARRESTS

A citizen's arrest, or a private person arresting another, is authorized under UCA 77-7-3.

- (a) A private person may arrest another:
 - 1. For a public offense committed or attempted in his/her presence.
 - 2. When a felony has been committed and he/she has reasonable cause to believe the person arrested has committed it. UCA 77-7-3.
- (b) Utah law requires a citizen making an arrest to take the arrested person before a magistrate or deliver him/her to a peace officer without delay.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Arrest With or Without a Warrant

1. Officers are not required to accept the arrested person but must make an independent judgment of the situation.
 2. In such cases, officers shall first determine the legality of the arrest.
 3. If the officer finds that probable cause exists, he/she can take custody of the arrested and take him/her before a magistrate.
 4. If he/she does not find probable cause, he/she shall advise the citizen to proceed directly to a magistrate or to the prosecutors office.
- (c) An officer who determines that a citizen's arrest is lawful may take one of the following courses of action:
1. Accepting custody and transporting:
 - (a) Before the officer accepts custody, the arresting person must complete a witness statement articulating the facts supporting probable cause for the citizens arrest.
 - (b) The officer may accept custody, but release the arrested person on a misdemeanor citation, subject to the standard requirements of the citation.
 - (c) Whenever possible, the officer should issue a misdemeanor citation, and have the arresting person co-sign the citation, and thereby avoid booking the prisoner.
- (d) Off-duty Peace Officer arrests:
- (a) Officers shall use good judgment and discretion when making off-duty arrests.
 - (b) Officers shall respond, at any time, to an emergency requiring an arrest, particularly if a crime of violence is involved.
 - (c) Arrests for minor misdemeanors, neighborhood disputes, and domestic disturbances are discouraged unless the circumstances are so severe that arrest is unavoidable.
 - (d) In such instances, officers shall call an on-duty officer to handle the matter.

901.5 PROCEDURES

- (a) When an arrest is affected on a South Salt Lake Justice Court warrant, the following alternative courses of action may be available. The alternatives are listed below in the order of preference:
1. If the Justice Court is in session, take the defendant before the court without necessary delay.
 2. If the defendant is able to post bond and the municipal court clerk's office is open for business, take the defendant before the court clerk to post bond.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Arrest With or Without a Warrant

3. If the defendant is unable to post bond, the officer may transport the prisoner to the Salt Lake County Jail or other facility for incarceration.
 - (a) Prior to transporting to jail, call the jail. If they refuse to take the defendant, include the name of the person refusing custody in a follow-up report.
 - (b) The officer preparing the custody forms will obtain copies of the warrant from the records section and attach a warrant copy to the custody forms submitted to the jail and the custody forms retained by this department.
 - (c) A copy of the custody form becomes the return for the warrant, and will contain the date and time served, name of server, to whom process was served or on whom executed, method of service, and location of service.

Alternative to Arrest

902.1 PURPOSE AND SCOPE

- (a) Officers of the South Salt Lake City Police Department, when attempting to resolve the various types of problems to which they respond, are encouraged to seek alternatives to physical arrest (with incarceration) when no hazard(s) to the community, the victim or suspect will result. This department is allowed the use of discretion within the guidelines of department standards, statutory and case law, and to some extent, prevailing community standards.
 - 1. Officers will exercise arrest powers in felony situations. Dependent upon the felony offense (non-hazardous) and prosecutorial approval, certain felony arrestees may be released pending arraignment, after interview, without being formally incarcerated.
 - 2. Officers may exercise the concept of "verbal warning" on those traffic and simple misdemeanor offenses where the facts indicate proper resolution of the event can be achieved without formal charge.
 - 3. A supervisor or department administration may restrict this discretionary action or selective traffic enforcement, in those areas of directed patrol requiring stricter attention to enforcement or where community need warrants formal charges.
 - 4. Officers should not use the "verbal warning" to evade resolving the situation properly.
 - 5. Supervisors will ensure that each incident response and resolution by police officers is properly documented as directed by applicable standards and orders.
- (b) Certain situations require the physical arrest and incarceration of a crime suspect, either by law or by virtue of the circumstances confronting the officer(s) at the time of the contact. Many other contacts however, do not require a physical arrest and incarceration, and should thus be handled through the implementation of an appropriate alternative:
 - 1. Detention/Holding - Generally used in cases involving juveniles who may not be incarcerated, while awaiting disposition or acceptance by a juvenile holding facility, release to parent(s), relative, or a responsible adult.
 - 2. Misdemeanor Citations - Officers shall use misdemeanor citations in lieu of arrest for persons charged with misdemeanors under most circumstances, when the person can be identified beyond reasonable doubt and has been a local resident for at least six months.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Alternative to Arrest

- (a) If the person has outstanding warrants, may be chargeable for multiple offenses, or the original charge might escalate into a felony, then a custodial arrest is required.
- (b) An arresting officer may issue a citation to appear at a time and place specified in the citation whenever any person is detained by or in the custody of an arresting officer for a misdemeanor infraction charge 77-7-18.
- (c) Anything in this subsection to the contrary notwithstanding, if the arresting officer believes that (1) any person is likely to disregard a citation, or (2) is likely to cause harm to him/herself or to any other person, then the person should be brought forthwith before a magistrate, and the procedure for warrant-less arrest, shall be followed.

3. Diversion

- (a) The South Salt Lake City Police Department is not directly or indirectly involved with any organized diversion programs. However, the South Salt Lake City Police officers may use their discretion and divert a juvenile offender to his/her parent(s), guardian(s), school, etc., if the officer feels that the juvenile, the department and the community are best served by doing this. The officer must consider the following factors when making a decision to divert:
 - 1. Has the juvenile committed any other offenses in the past?
 - 2. If so, what type of crime(s) did the juvenile commit?
 - 3. How serious was the nature of the crime(s) committed?

902.1.1 OFFICER DISCRETION

The purpose of establishing limits to the officer's discretionary powers is to eliminate discriminatory enforcement of the law and to protect the officer by establishing policy governing certain enforcement situations.

While most circumstances require department personnel to adhere to department policies and procedures to the best of their ability, it is also recognized that no policy or procedure can be adopted that will cover the particulars of every circumstance.

With this in mind, it shall be the policy of this department that sworn personnel are given the authority and responsibility to employ individual judgment and discretion in those circumstances where strict adherence to procedure would be to the obvious detriment of the public or the department. Personnel deviating from such procedure should make every attempt to notify a supervisor prior to such deviation taking place.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Alternative to Arrest

- (a) Reasonable and appropriate police action varies with each situation. Different facts or circumstances may justify an investigation, a detention, a search, an arrest, or no action at all. Department employees must continually exercise discretionary judgment, in order to ensure that the safety of the public is properly protected.
- (b) Department employees shall exercise discretionary judgment in a reasonable manner and shall limit such judgment within the confines directed by:
 - 1. The oath of office.
 - 2. The confines of authority as described by law.
 - 3. The decisions and interpretations established by judicial bodies.
 - 4. The written directives of the Police Department and the City of South Salt Lake.
 - 5. Verbal direction of a supervisor.
- (c) Sworn employees of the department are required to initiate investigative action when allegations for violations of the ordinances of South Salt Lake City, laws of the State of Utah and the United States come to their attention. Such actions by sworn employees shall be conducted with the restrictions established by departmental directives and may range in scope from referral to the appropriate agency to the arrest of the violator.
- (d) Enforcement action shall be expected of all sworn employees of the department while on duty when one or any of the following criteria exists:
 - 1. All the elements of a crime exist.
 - 2. Probable cause exists indicating the suspect committed the offense.
 - 3. All departmental policies and procedures are complied with.
 - 4. A willing complainant requesting police action or the officer observes the crime.
 - 5. Enforcement action may be based upon UCA 77-7-18.
- (e) Unless directed by other departmental regulations or law, the officer may conclude police incidents by informal disposition. Informal disposition includes referral to another agency, agreement among affected parties and warning.
- (f) In the officer's decision-making process to initiate enforcement action or upon arrest, the decision for continued physical custody shall not be based upon:
 - 1. The attitude of the subject of arrest, including the subject's disrespect toward law enforcement.
 - 2. The subject's race, creed, color, sex, or religious, ethnic or national origin.

Temporary Detention by Private Persons

903.1 PURPOSE AND SCOPE

This policy provides guidance for the handling and acceptance of an individual temporarily detained by a private person.

903.2 POLICY

It is the policy of the South Salt Lake Police Department to arrest an individual who has been temporarily detained by a private person only when legal and appropriate.

903.3 TEMPORARY DETENTIONS BY PRIVATE PERSONS

A private person may temporarily detain another under the following circumstances (Utah Code 77-7-3):

- (a) A public offense is committed or attempted in the private person's presence.
- (b) A felony has been committed, and the private person has reasonable cause to believe the individual being detained has committed it.
 - 1. Private persons may not detain an individual on suspicion that a felony has been committed. The felony must in fact have taken place.

For a temporary detention by a private person to be lawful, the private person must immediately notify law enforcement of the situation and the temporary detention unless they know another person has already done so, and the temporary detention lasts only until officers arrive (Utah Code 77-7-3).

903.4 OFFICER RESPONSIBILITIES

An officer confronted with a person claiming to have temporarily detained an individual should determine whether such a detention is lawful (Utah Code 77-7-7.1).

If the officer determines that the temporary detention is unlawful, the officer should:

- (a) Take no action to further detain or restrain the individual unless there is independent justification for continuing a detention.
- (b) Advise the parties that the detention will not be accepted but the circumstances will be documented in a report.
- (c) Document the incident, including the basis for refusing to accept custody of the individual.

Whenever an officer determines that a temporary detention by a private person is lawful, the officer may take the individual into custody and proceed in the same manner as with any other arrest (Utah Code 77-7-7.1)

903.5 PRIVATE PERSON'S TEMPORARY DETENTION FORM

The private person claiming to have made a temporary detention should be asked to complete and sign a private person's temporary detention form. If the person fails or refuses to do so, the

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Detention by Private Persons

detained individual should be released, unless the officer has a lawful reason, independent of the private person's temporary detention, to take the individual into custody and determines an arrest is appropriate.

See attachment: [Private Persons Temporary Detention Form.pdf](#)

Arrest or Detention of Foreign Nationals

904.1 PURPOSE AND SCOPE

This policy provides guidelines to ensure that members of the South Salt Lake Police Department extend appropriate privileges and immunities to foreign diplomatic and consular representatives in accordance with international law.

904.2 POLICY

The South Salt Lake Police Department respects international laws related to the special privileges and immunities afforded foreign diplomatic and consular representatives assigned to the United States.

All foreign diplomatic and consular representatives shall be treated with respect and courtesy, regardless of any privileges or immunities afforded them.

904.3 CLAIMS OF IMMUNITY

If a member comes into contact with a person where law enforcement action may be warranted and the person claims diplomatic or consular privileges and immunities, the member should, without delay:

- (a) Notify a supervisor.
- (b) Advise the person that his/her claim will be investigated and he/she may be released in accordance with the law upon confirmation of the person's status.
- (c) Request the person's identification card, either issued by the U.S. Department of State (DOS), Office of the Chief of Protocol, or in the case of persons accredited to the United Nations, by the U.S. Mission to the United Nations. These are the only reliable documents for purposes of determining privileges and immunities.
- (d) Contact the DOS Diplomatic Security Command Center at 571-345-3146 or toll free at 866-217-2089, or at another current telephone number and inform the center of the circumstances.
- (e) Verify the immunity status with DOS and follow any instructions regarding further detention, arrest, prosecution and/or release, as indicated by the DOS representative. This may require immediate release, even if a crime has been committed.

Identity or immunity status should not be presumed from the type of license plates displayed on a vehicle. If there is a question as to the status or the legitimate possession of a Diplomat or Consul license plate, a query should be run via the National Law Enforcement Telecommunications System (NLETS), designating "US" as the state.

904.4 ENFORCEMENT ACTION

If the DOS is not immediately available for consultation regarding law enforcement action, members shall be aware of the following:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Arrest or Detention of Foreign Nationals

- (a) Generally, all persons with diplomatic and consular privileges and immunities may be issued a citation or notice to appear. However, the person may not be compelled to sign the citation.
- (b) All persons, even those with a valid privilege or immunity, may be reasonably restrained in exigent circumstances for purposes of self-defense, public safety or the prevention of serious criminal acts.
- (c) An impaired foreign diplomatic or consular representative may be prevented from driving a vehicle, even if the person may not be arrested due to privileges and immunities.
 - 1. Investigations, including the request for field sobriety tests, chemical tests and any other tests regarding impaired driving may proceed but they shall not be compelled.
- (d) The following persons may not be detained or arrested, and any property or vehicle owned by these persons may not be searched or seized:
 - 1. Diplomatic-level staff of missions to international organizations and recognized family members
 - 2. Diplomatic agents and recognized family members
 - 3. Members of administrative and technical staff of a diplomatic mission and recognized family members
 - 4. Career consular officers, unless the person is the subject of a felony warrant
- (e) The following persons may generally be detained and arrested:
 - 1. International organization staff; however, some senior officers are entitled to the same treatment as diplomatic agents.
 - 2. Support staff of missions to international organizations
 - 3. Diplomatic service staff and consular employees; however, special bilateral agreements may exclude employees of certain foreign countries
 - 4. Honorary consular officers

904.5 DOCUMENTATION

All contacts with persons who have claimed privileges and immunities afforded foreign diplomatic and consular representatives should be thoroughly documented and the related reports forwarded to DOS.

904.5.1 DOCUMENTATION PROCEDURES

An officer who stops a person holding a driver's license issued by the DOS or otherwise claiming privileges or immunities, for a moving traffic violation or any of the following offenses while operating a vehicle shall document all of the relevant information from the driver's license or identification card (Utah Code 41-6a-1901):

- (a) Automobile homicide
- (b) Manslaughter

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Arrest or Detention of Foreign Nationals

- (c) Negligent homicide
- (d) Aggravated assault
- (e) Reckless endangerment

The Records Section shall forward such information with a copy of the traffic citation, vehicle accident report, or written report of the incident, as applicable, to the Department of Public Safety (DPS) within five working days (Utah Code 41-6a-1901).

904.6 DIPLOMATIC IMMUNITY TABLE

Reference table on diplomatic immunity:

Category	Arrested or	Enter	Issued	Subpoenaed	Prosecuted	Recognized
Diplomatic	No (note (b))	No	Yes	No	No	Same as sponsor (full immunity & inviolability)
Member of	No (note (b))	No	Yes	No	No	Same as sponsor (full immunity & inviolability)
Service Staff	Yes (note (a))	Yes	Yes	Yes	No for official acts Yes otherwise (note (a))	No immunity or inviolability (note (a))
Career	Yes if for a felony and pursuant to a warrant (note (a))	Yes (note (d))	Yes	No for official acts Testimony may not be compelled in any case	No for official acts Yes otherwise (note (a))	No immunity or inviolability
Honorable	Yes	Yes	Yes	No for official acts Yes otherwise	No for official acts Yes otherwise (note (a))	No immunity or inviolability
Consulate	Yes (note (a))	Yes	Yes	No for official acts Yes otherwise	No for official acts Yes otherwise (note (a))	No immunity or inviolability (note (a))
Int'l Org	Yes (note (c))	Yes (note (c))	Yes	Yes (note (c))	No for official acts Yes otherwise (note (c))	No immunity or inviolability

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Arrest or Detention of Foreign Nationals

Diplomatic-	No (note (b))	No	Yes	No	No	Same as sponsor (full immunity and inviolability)
Support	Yes	Yes	Yes	Yes	No for official act Yes otherwise	No immunity or inviolability

Notes for diplomatic immunity table:

- (a) This table presents general rules. The employees of certain foreign countries may enjoy higher levels of privileges and immunities on the basis of special bilateral agreements.
- (b) Reasonable constraints, however, may be applied in emergency circumstances involving self-defense, public safety, or in the prevention of serious criminal acts.
- (c) A small number of senior officers are entitled to be treated identically to diplomatic agents.
- (d) Note that consul residences are sometimes located within the official consular premises. In such cases, only the official office space is protected from police entry.

Temporary Custody of Juveniles

905.1 PURPOSE AND SCOPE

This policy provides guidelines consistent with the Juvenile Justice and Delinquency Prevention Act for juveniles taken into temporary custody by members of the South Salt Lake Police Department (34 USC § 11133).

905.1.1 DEFINITIONS

Definitions related to this policy include:

Juvenile non-offender - An abused, neglected, dependent, or alien juvenile who may be legally held for the juvenile's own safety or welfare. This also includes any juvenile who may have initially been contacted for an offense that would not subject an adult to arrest (e.g., fine-only offense) but was taken into custody for the juvenile's protection or for purposes of reuniting the juvenile with a parent, guardian, or other responsible person. Juveniles engaged in commercial sex or sexual solicitation are non-offenders (Utah Code 76-5d-106; Utah Code 76-5d-204; Utah Code 76-5d-209; Utah Code 76-5d-211).

Juvenile offender - A juvenile under 18 who is alleged to have committed an offense that would subject an adult to arrest (a non-status offense). It also includes possession of a handgun by a person under 18 years of age in violation of Utah Code 76-11-211 (28 CFR 31.303).

Non-secure custody - When a juvenile is held in the presence of an officer or other [department/office] member at all times and is not placed in a locked room, cell, or behind any locked doors. Juveniles in non-secure custody may be handcuffed but not to a stationary or secure object. Personal supervision, through direct visual monitoring and audio two-way communication, is maintained. Monitoring through electronic devices, such as video, does not replace direct visual observation.

Safety checks - Direct visual observation by a member of this [department/office] performed at random intervals, within time frames prescribed in this policy, to provide for the health and welfare of juveniles in temporary custody.

Secure custody - When a juvenile offender is held in a locked room, a set of rooms, or a cell. Secure custody also includes being physically secured to a stationary object.

Examples of secure custody include:

- (a) A juvenile left alone in an unlocked room within the secure perimeter of the adult temporary holding area.
- (b) A juvenile handcuffed to a rail.
- (c) A juvenile placed in a room that contains doors with delayed egress devices that have a delay of more than 30 seconds.
- (d) A juvenile being processed in a secure booking area when a non-secure booking area is available.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Custody of Juveniles

- (e) A juvenile left alone in a secure booking area after being photographed and fingerprinted.
- (f) A juvenile placed in a cell within the adult temporary holding area, whether or not the cell door is locked.
- (g) A juvenile placed in a room that is capable of being locked or contains a fixed object designed for cuffing or restricting movement.

Sight and sound separation - Located or arranged to prevent physical, visual, or auditory contact.

Status offender - A juvenile suspected of committing a criminal violation of the law that would not be a criminal violation but for the age of the offender. Examples may include running away, underage possession of tobacco, curfew violation, and truancy. A juvenile in custody on a court order or warrant based upon a status offense is also a status offender.

905.2 POLICY

The South Salt Lake Police Department is committed to releasing juveniles from temporary custody as soon as reasonably practicable and to keeping juveniles safe while in temporary custody at the South Salt Lake Police Department. Juveniles should be held in temporary custody only for as long as reasonably necessary for processing, transfer, or release.

905.3 JUVENILES WHO SHOULD NOT BE HELD

Juveniles who exhibit certain behaviors or conditions should not be held at the South Salt Lake Police Department. These include:

- (a) Unconsciousness or having been unconscious while being taken into custody or transported.
- (b) Serious injuries or a medical condition requiring immediate medical attention.
- (c) A suspected suicide risk or showing obvious signs of severe emotional or mental disturbance (see the Involuntary Commitments Policy).
 - 1. If the officer taking custody of a juvenile believes that the juvenile may be a suicide risk, the officer shall ensure continuous direct supervision until evaluation, release, or transfer to an appropriate facility is completed.
- (d) Significant intoxication or showing signs of having ingested any substance that poses a significant risk to their health, whether or not they appear intoxicated.
- (e) Extremely violent or continuously violent behavior.
- (f) Afflicted with, or displaying symptoms of, a communicable disease that poses an unreasonable exposure risk.

Officers taking custody of a juvenile exhibiting any of the above conditions should take reasonable steps to provide medical attention or mental health assistance and should notify a supervisor of the situation. These juveniles should not be held at the South Salt Lake Police Department unless they have been evaluated by a qualified medical and/or mental health professional, as appropriate for the circumstances.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Custody of Juveniles

905.4 CUSTODY OF JUVENILES

Officers should take custody of a juvenile and temporarily hold the juvenile at the South Salt Lake Police Department when there is no other lawful and practicable alternative to temporary custody. Refer to the Child Abuse Policy for additional information regarding detaining a juvenile who is suspected of being a victim.

No juvenile should be held in temporary custody at the South Salt Lake Police Department without authorization of the arresting officer's supervisor or the Watch Commander. Juveniles taken into custody shall be held in non-secure custody unless otherwise authorized by this policy.

Any juvenile taken into custody shall be released to the care of the juvenile's parent, legal guardian, or other responsible adult, or transferred to a juvenile custody facility or to other authority as soon as practicable, and in no event shall a juvenile be held beyond six hours from the time of the juvenile's entry into the South Salt Lake Police Department (34 USC § 11133; Utah Code 80-6-203; Utah Code 80-6-204).

905.4.1 CUSTODY OF JUVENILE NON-OFFENDERS

Non-offenders taken into protective custody in compliance with the Child Abuse Policy should generally not be held at the South Salt Lake Police Department. Custodial arrangements should be made for non-offenders as soon as reasonably possible. Juvenile non-offenders may not be held in secure custody (34 USC § 11133).

905.4.2 CUSTODY OF JUVENILE STATUS OFFENDERS

Status offenders should generally be released by citation or with a warning rather than taken into temporary custody. However, officers may take custody of a status offender if requested to do so by a parent or legal guardian in order to facilitate reunification (e.g., transported home or to the station to await a parent). Juvenile status offenders may not be held in secure custody (34 USC § 11133).

905.4.3 CUSTODY OF JUVENILE OFFENDERS

Juvenile offenders should be held in non-secure custody while at the South Salt Lake Police Department unless another form of custody is authorized by this policy or is necessary due to exigent circumstances.

A juvenile offender may be taken into custody without order of the court if the officer has probable cause to believe the juvenile has violated a state law, federal law, local law, or municipal ordinance (Utah Code 80-6-201).

A juvenile offender may not be held in temporary custody any longer than is reasonably necessary to obtain the juvenile's name, age, residence, and other necessary information, and to contact the juvenile's parents, guardian, or custodian (Utah Code 80-6-203).

The juvenile offender shall be released to the care of a parent or other responsible adult, unless the officer reasonably believes the juvenile's immediate welfare or the protection of the community requires the juvenile's detention or a warrant has been issued under Utah Code 80-6-202 or Utah Code 80-6-806 (Utah Code 80-6-203). Before releasing the juvenile offender, the parent or other

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Custody of Juveniles

person taking custody of the juvenile shall be required to sign a written promise to bring the juvenile to the court at the specified date and time (Utah Code 80-6-203).

If the juvenile offender is not released, the juvenile shall be taken to a place of detention or shelter without unnecessary delay (Utah Code 80-6-203).

The officer who takes a juvenile offender to a detention or shelter facility shall complete and promptly file with the detention or shelter facility a written report on a form provided by the Division of Juvenile Justice and Youth Services. This should include the details of the presently alleged offense, the facts that bring the juvenile within the jurisdiction of the juvenile court, the reason the juvenile was not released by the [Department/Office], and if the juvenile is under consideration for detention, the eligibility of the juvenile for detention under the detention guidelines (Utah Code 80-6-203).

905.5 ADVISEMENTS

If a juvenile offender is taken into custody under Utah Code 80-6-201 for a serious offense as defined by Utah Code 80-6-103, the officer should notify the appropriate school superintendent or principal or their designee within five days for the purposes of the juvenile's supervision and student safety. The notice shall disclose only (Utah Code 80-6-103):

- (a) The name of the juvenile.
- (b) The offense for which the juvenile was taken into custody or detention.
- (c) If available, the name of the victim, if the victim either resides in the same school district as the juvenile or attends the same school as the juvenile.

905.6 NO-CONTACT REQUIREMENTS

Sight and sound separation shall be maintained between all juveniles and adults while in custody at the [Department/Office] (34 USC § 11133; Utah Code 80-6-204). There should also be sight and sound separation between non-offenders and juvenile and status offenders.

In situations where brief or accidental contact may occur (e.g., during the brief time a juvenile is being fingerprinted and/or photographed in booking), a member of the South Salt Lake Police Department shall maintain a constant, immediate, side-by-side presence with the juvenile or the adult to minimize any contact. If inadvertent or accidental contact does occur, reasonable efforts shall be taken to end the contact.

905.7 TEMPORARY CUSTODY REQUIREMENTS

Members and supervisors assigned to monitor or process any juvenile at the South Salt Lake Police Department shall ensure:

- (a) The Watch Commander is notified if it is anticipated that a juvenile may need to remain at the South Salt Lake Police Department more than four hours. This will enable the Watch Commander to ensure no juvenile is held at the South Salt Lake Police Department more than six hours.
- (b) Safety checks and significant incidents/activities are noted on the log.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Custody of Juveniles

- (c) Juveniles in custody are informed that they will be monitored at all times, except when using the toilet.
 - 1. There shall be no viewing devices, such as peep holes or mirrors, of which the juvenile is not aware.
 - 2. This does not apply to surreptitious and legally obtained recorded interrogations.
- (d) A member of the same sex will supervise personal hygiene activities and care, such as changing clothing or using the restroom, without direct observation to allow for privacy.
- (e) There is reasonable access to toilets and wash basins.
- (f) There is reasonable access to a drinking fountain or water.
- (g) Food is provided if a juvenile has not eaten within the past four hours or is otherwise in need of nourishment, including any special diet required for the health of the juvenile.
- (h) There are reasonable opportunities to stand and stretch, particularly if handcuffed or otherwise restrained.
- (i) There is privacy during family, guardian, and/or attorney visits.
- (j) Juveniles are generally permitted to remain in their personal clothing unless it is taken as evidence or is otherwise unsuitable or inadequate for continued wear while in custody.
- (k) Clean blankets are provided as reasonably necessary to ensure the comfort of an individual.
 - 1. The supervisor should ensure that there is an adequate supply of clean blankets.
- (l) Adequate shelter, heat, light, and ventilation are provided without compromising security or enabling escape.
- (m) Adequate furnishings are available, including suitable chairs or benches.
- (n) Juveniles have the right to the same number of telephone calls as adults in temporary custody (see the Temporary Custody of Adults Policy).
- (o) Discipline is not administered to any juvenile, nor will juveniles be subjected to corporal or unusual punishment, humiliation, or mental abuse.

905.8 USE OF RESTRAINT DEVICES

Juvenile offenders may be handcuffed in accordance with the Handcuffing and Restraints Policy. A juvenile offender may be handcuffed at the South Salt Lake Police Department when the juvenile presents a heightened risk. However, non-offenders and status offenders should not be handcuffed unless they are combative or threatening.

Other restraints shall only be used after less restrictive measures have failed and with the approval of the Watch Commander. Restraints shall only be used so long as it reasonably appears necessary for the juvenile's protection or the protection of others.

Juveniles in restraints shall be kept away from other unrestrained individuals in custody and monitored to protect them from abuse.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Custody of Juveniles

905.8.1 PREGNANT JUVENILES

Juveniles who are known to be pregnant should be restrained in accordance with the Handcuffing and Restraints Policy.

905.9 PERSONAL PROPERTY

The personal property of a juvenile shall be processed in the same manner as an adult in temporary custody (see the Temporary Custody of Adults Policy).

905.10 SUICIDE ATTEMPT, DEATH, OR SERIOUS INJURY OF A JUVENILE

The Patrol Division Commander will ensure procedures are in place to address the suicide attempt, death, or serious injury of any juvenile held at the South Salt Lake Police Department. The procedures should include the following:

- (a) Immediate request for emergency medical assistance if appropriate
- (b) Immediate notification of the Watch Commander, Chief of Police, and Investigation Division Commander
- (c) Notification of the parent, guardian, or person standing in loco parentis of the juvenile
- (d) Notification of the appropriate prosecutor
- (e) Notification of the City Attorney
- (f) Notification of the Medical Examiner
- (g) Notification of the juvenile court
- (h) Evidence preservation

905.11 INTERVIEWING OR INTERROGATING

No interview or interrogation of a juvenile should occur unless the juvenile has the apparent capacity to consent, and does consent, to an interview or interrogation.

No interrogation of a juvenile should occur unless (Utah Code 80-6-206):

- (a) The juvenile has been advised of the juvenile's constitutional rights, and the right to have a parent, a guardian, or a friendly adult present during the interrogation.
- (b) The juvenile voluntarily waives the juvenile's constitutional rights.
- (c) A parent, guardian, or friendly adult is present during the interrogation or gives consent to the interrogation after being present for the waiver. A parent, guardian, or friendly adult is not required to be present for the waiver or give consent if reasonable attempts to contact such an individual have been unsuccessful for one hour after taking the juvenile into custody or if the juvenile's attorney is present in accordance with (d) below.
- (d) When being held in a detention facility or a secure care facility, the juvenile has had a meaningful opportunity to consult with their attorney and the attorney is present for the interrogation.
- (e) The juvenile's guardian ad litem, if any, has given consent to the interrogation for a juvenile who is in the custody of the Division of Child and Family Services.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Custody of Juveniles

Any custodial interrogation of a juvenile should be recorded (audio or video with audio as available) in its entirety (Utah Code 80-6-206).

905.11.1 CONDUCT OF INTERVIEW OR INTERROGATION

An officer shall not provide false information about evidence that is reasonably likely to elicit an incriminating response, nor shall an officer make unauthorized statements about leniency for the offense being investigated.

905.12 RESTRICTION ON FINGERPRINTING AND PHOTOGRAPHING

An officer should not photograph or fingerprint a juvenile who has not been adjudicated of an offense (Utah Code 80-6-608).

905.13 RECORDS

Court decisions and legislation have combined to carefully specify situations in which information may be given out or exchanged when a case involves a minor. Juvenile record disclosures are governed by Utah Code, Title 63G, Chapter 2, Government Records Access and Management Act (GRAMA) and the federal Family Educational Rights and Privacy Act (FERPA) (Utah Code 80-6-103).

Officers shall not divulge any information regarding juveniles in situations where they are uncertain of the legal authority to do so.

Only information authorized by law will be released to other agencies. It shall be the responsibility of the Records Supervisor and the appropriate Investigation Division supervisors to ensure that personnel of those bureaus act within legal guidelines.

905.14 RELIGIOUS ACCOMMODATION

Juveniles have the right to the same religious accommodation as adults in temporary custody (see the Temporary Custody of Adults Policy).

905.15 TRAINING

Members should be trained on and familiar with this policy and any supplemental procedures.

Custodial Searches

906.1 PURPOSE AND SCOPE

This policy provides guidance regarding searches of individuals in custody. Such searches are necessary to eliminate the introduction of contraband, intoxicants, or weapons into the South Salt Lake Police Department facility. Such items can pose a serious risk to the safety and security of [department/office] members, individuals in custody, contractors, and the public.

Guidance for custody searches when transporting a person in custody may be found in the Transporting Persons in Custody Policy.

Nothing in this policy is intended to prohibit the otherwise lawful collection of evidence from an individual in custody.

906.1.1 DEFINITIONS

Definitions related to this policy include:

Custody search - An in-custody search of an individual and of his/her property, shoes and clothing, including pockets, cuffs and folds on the clothing, to remove all weapons, dangerous items and contraband.

Physical body cavity search - A search that includes a visual inspection and may include a physical intrusion into a body cavity. Body cavity means the stomach or rectal cavity of an individual, and the vagina of a female person.

Strip search - A search that requires an individual to remove or rearrange some or all of his/her clothing to permit a visual inspection of the underclothing, breasts, buttocks, anus or outer genitalia. This includes monitoring an individual who is changing clothes, where his/her underclothing, buttocks, genitalia or female breasts are visible.

906.2 POLICY

All searches shall be conducted with concern for safety, dignity, courtesy, respect for privacy and hygiene, and in compliance with policy and law to protect the rights of those who are subject to any search.

Searches shall not be used for intimidation, harassment, punishment or retaliation.

906.3 SEARCHES AT PUBLIC SAFETY FACILITIES

South Salt Lake Police Department An officer should conduct a custody search of an individual immediately after arrest, when receiving an individual from custody of another, and before transporting a person who is in custody in any City owned vehicle. Custody searches shall be conducted on all individuals in custody, upon entering a City owned vehicle or facilities. Except in exigent circumstances, the search should be conducted by a member of the same sex as the individual being searched. If a member of the same sex is not available, a witnessing member must be present during the search. BWC and Dash Camera should capture the search.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Custodial Searches

Custody searches should also be conducted any time an individual in custody enters or re-enters a secure area, or any time it is reasonably believed that a search is necessary to maintain the safety and security of the facility.

906.3.1 PROPERTY

Members shall take reasonable care in handling the property of an individual in custody to avoid discrepancies or losses. Property retained for safekeeping shall be kept in a secure location until the individual is released or transferred.

Some property may not be accepted by a facility or agency that is taking custody of an individual from this [department/office], such as weapons or large items. These items should be retained for safekeeping in accordance with the Property and Evidence Policy.

All property shall be inventoried by objective description (this does not include an estimated value). The individual from whom it was taken shall be required to sign the completed inventory. If the individual's signature cannot be obtained, the inventory shall be witnessed by another [department/office] member. The inventory should include the case number, date, time, member's South Salt Lake Police Department identification number, and information regarding how and when the property may be released.

906.3.2 VERIFICATION OF MONEY

All money shall be counted in front of the individual from whom it was received. When possible, the individual shall initial the dollar amount on the inventory. Additionally, all money should be placed in a separate envelope and sealed. Negotiable checks or other instruments and foreign currency should also be sealed in an envelope with the amount indicated but not added to the cash total. All envelopes should clearly indicate the contents on the front. The [department/office] member sealing it should place their initials across the sealed flap. Should any money be withdrawn or added, the member making such change shall enter the amount below the original entry and initial it. The amount of money in the envelope should always be totaled and written on the outside of the envelope.

906.4 STRIP SEARCHES

No individual in temporary custody at any South Salt Lake Police Department facility shall be subjected to a strip search unless there is reasonable suspicion based upon specific and articulable facts to believe the individual has a health condition requiring immediate medical attention or is concealing a weapon or contraband. Factors to be considered in determining reasonable suspicion include but are not limited to:

- (a) The detection of an object during a custody search that may be a weapon or contraband and cannot be safely retrieved without a strip search.
- (b) Circumstances of a current arrest that specifically indicate the individual may be concealing a weapon or contraband.
 - 1. A felony arrest charge or being under the influence of a controlled substance should not suffice as reasonable suspicion absent other facts.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Custodial Searches

- (c) Custody history (e.g., past possession of contraband while in custody, assaults on [department/office] members, escape attempts).
- (d) The individual's actions or demeanor.
- (e) Criminal history (i.e., level of experience in a custody setting).

No transgender or intersex individual shall be searched or examined for the sole purpose of determining the individual's genital status. If the individual's genital status is unknown, it may be determined during conversations with the person, by reviewing medical records, or as a result of a broader medical examination conducted in private by a medical practitioner (28 CFR 115.115).

906.4.1 STRIP SEARCH PROCEDURES

Strip searches at South Salt Lake Police Department facilities shall be conducted as follows (28 CFR 115.115):

- (a) Written authorization from the Watch Commander shall be obtained prior to the strip search.
- (b) All members involved with the strip search shall be of the same sex as the individual being searched, unless the search is conducted by a medical practitioner.
- (c) All strip searches shall be conducted in a professional manner under sanitary conditions and in a secure area of privacy so that it cannot be observed by those not participating in the search. The search shall not be reproduced through a visual or sound recording.
- (d) Whenever possible, a second member of the same sex should also be present during the search, for security and as a witness to the finding of evidence.
- (e) Members conducting a strip search shall not touch the breasts, buttocks or genitalia of the individual being searched.
- (f) The primary member conducting the search shall prepare a written report to include:
 - 1. The facts that led to the decision to perform a strip search.
 - 2. The reasons less intrusive methods of searching were not used or were insufficient.
 - 3. The written authorization for the search, obtained from the Watch Commander.
 - 4. The name of the individual who was searched.
 - 5. The name and sex of the members who conducted the search.
 - 6. The name, sex and role of any person present during the search.
 - 7. The time and date of the search.
 - 8. The place at which the search was conducted.
 - 9. A list of the items, if any, that were recovered.
 - 10. The facts upon which the member based his/her belief that the individual was concealing a weapon or contraband.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Custodial Searches

- (g) No member should view an individual's private underclothing, buttocks, genitalia or female breasts while that individual is showering, performing bodily functions or changing clothes, unless he/she otherwise qualifies for a strip search. However, if serious hygiene or health issues make it reasonably necessary to assist the individual with a shower or a change of clothes, a supervisor should be contacted to ensure reasonable steps are taken to obtain the individual's consent and/or otherwise protect his/her privacy and dignity.

906.4.2 TRANSPORT VEHICLE SEARCH

- (a) Prior to utilizing any assigned police vehicle each officer shall inspect the vehicle to ensure that contraband, weapons, and/or dangerous mechanical conditions are not present.
- (b) A search of the police vehicle for weapons and/or contraband shall be conducted immediately before and after each prisoner transport.
- (c) In the event that contraband or weapons are located during the beginning of shift search, the assigned officer shall notify the supervisor on-duty or in his/her absence, the on-duty watch commander.
 - 1. Every effort should be made to determine if the contraband and/or weapon is evidence.
 - 2. If so, the items will be processed as evidence and the appropriate supplement report will be written.
 - 3. If the items are not evidence, they will be processed as "found property."
- (d) Prior to operating a police vehicle for a shift or transport, the officer shall ensure the vehicle is operating properly, and that the equipment necessary for emergency road repairs is available and in good working order.
 - 1. The inspection shall include the confirming the presence of flares and first aid kits.
 - 2. Additionally, fluid levels shall be checked at each gasoline fill-up, and the officer should have means to obtain fuel and operational fluids.
 - 3. The officer shall report any police vehicle mechanical condition to his/her supervisor and make arrangements to transport the vehicle to the city shop to correct the problem as soon as possible.

906.4.3 SECURITY OF TRANSPORTING OFFICER - GUIDELINES

- (a) Normally, a barrier-equipped vehicle should be used for transporting prisoners.
 - 1. The prisoner will be secured beyond the access of the transporting officer in control of the vehicle.
 - 2. The barrier should be located between the front and rear seat compartments.
- (b) Transport vehicles should have the rear window cranks and door handles removed or disabled. Electric door locks, if present, will only be operable from the driver's compartment.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Custodial Searches

- (c) If a non-barrier equipped vehicle is utilized for transport, a single prisoner should be secured in the right front seat in such a manner that he/she cannot reasonably become a hazard to the officer in control of the vehicle.
- (d) The transporting officer shall utilize additional officers as necessary to ensure prisoner supervision and prevention of escape.
 - 1. The additional officer shall seat him/herself directly behind the prisoner being transported.
 - 2. If two prisoners are transported in the same vehicle, one will be secured in the right front seat and one in the right rear seat, and the additional officer will seat him/herself in the left rear seat directly behind the vehicle operator.

906.4.4 EXTENDED PRISONER TRANSPORT - GUIDELINES

- (a) During lengthy transports, prisoners shall be afforded the opportunity to use toilet facilities only after the officer is satisfied that adequate security can be maintained.
- (b) In the event of a long transport, such as during an extradition, transporting officers may allow meals for the prisoner.
 - 1. Selection of the type of meal and the location of the eating facility should be random to diminish the likelihood of escape.
 - 2. Feeding prisoners in transit may require summoning assistance from other agencies to ensure adequate security.
 - 3. Whenever possible, this will be arranged in advance of the transport.
- (c) In the event that it is necessary to transport a prisoner via commercial transportation, meals will be provided in conjunction with the carrier's regular schedule. Officers will continue to ensure that food and eating utensils are not capable of being used as weapons, and that the best possible security is maintained.
- (d) An officer transporting any prisoner has the primary responsibility of the safe delivery of that prisoner.
 - 1. A transport should not be interrupted to render police services.
 - 2. Only in situations where there is grave and imminent danger to third parties and assistance can be rendered with a minimum of danger to the prisoner, may an officer stop to render police service.
 - 3. Any such interruption will require that the transporting officer notify communications as to his/her location and the nature of his/her activity.
 - 4. Officers should use extreme caution in these situations, in that the perceived incident may in fact be a ruse for the prisoner to escape.

906.4.5 COMMUNICATION WITH PRISONER DURING TRANSPORT

- (a) Due to the difficulty in providing security and safety to the public, the prisoner and the transporting officer, a prisoner in transit to or from custodial facilities, will not be allowed to communicate with others.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Custodial Searches

1. The transporting officer shall deny all requests for such communication.
2. The transporting officer may explain the following to persons requesting communication with the prisoner:
 - (a) The destination of the prisoner.
 - (b) The availability or lack of visitor facilities at the destination.
 - (c) Whether the prisoner will have access to a telephone at the destination.
 - (d) Any other information pertinent to the availability of the prisoner for communication at the destination.

906.4.6 TRANSPORTING A PRISONER TO A FACILITY

- (a) Any officer transporting a prisoner to another facility shall comply with the regulations of that facility.
 1. The officer shall secure his/her weapon prior to allowing a prisoner to exit the vehicle, when security storage is made available.
 2. Officers will secure their weapons before entering any security perimeter of any facility.
 3. Handcuffs or other restraining devices shall not be removed until the prisoner is within the security perimeter of that facility.
- (b) Any officer transporting a prisoner from one facility to another shall provide all documents required by the accepting facility, and will further provide any special notations on the prisoner's health, behavior, potential for escape, or propensity to violence.
- (c) Any officer relinquishing custody of a prisoner to a facility shall obtain the receiving officer's signature.
- (d) If the transporting officer has property belonging to the prisoner, either the prisoner or the receiving officer must sign the property release section of the property receipt.

906.4.7 PRISONER ESCAPE DURING TRANSPORT

- (a) In the event a prisoner escapes while being transported, the transporting officer shall:
 1. Immediately notify communications of such occurrence and provide at least the following information:
 - (a) The location of the escape and the prisoner's last direction and method of travel.
 - (b) What the prisoner was in custody for, and if the prisoner is a danger to the public, him/herself, or others.
 - (c) A complete physical description of the prisoner including any clothing.
 2. Make every attempt to immediately return the prisoner to custody, if it is safe and practical to do so.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Custodial Searches

3. Request assistance and coordinate the placement and activities of responding units through the supervisor.
 4. Advise the on-duty supervisor of any information which will assist in determining other department resources the supervisor may want to utilize.
 5. Prepare the necessary reports concerning the incident to include case/crime reports, prosecutor forms, teletypes, and patrol information sheets.
- (b) If the prisoner is recaptured, the transporting or arresting officer shall additionally process the prisoner through another booking on escape charges, if appropriate.
- (a) Immediately notify communications to make the appropriate notifications to surrounding agencies.
- (c) In the event a prisoner escapes while being transported in another jurisdiction, the transporting officer shall:
- (a) Immediately notify the local or statewide dispatcher of the occurrence.
 - (b) Notify the local jurisdiction he/she is in, by using the primary or statewide radio frequency and request appropriate aid from the local jurisdiction.
 - (c) Make every effort to immediately return the prisoner to custody, if it is safe and practical to do so.
 - (d) Notify the on-duty supervisor, as well as, the Division Commanders as soon as possible.
 - (e) Assist the jurisdiction in which the escape took place by:
 - (a) Providing all information concerning the escape, including descriptions, reason for in-custody status, possible destinations, etc.
 - (b) Preparing any necessary reports requested by such jurisdiction.
 - (c) Prepare the necessary reports for this department, concerning the incident to include: case reports, prosecutor forms, teletypes, and patrol information sheets.
- (d) In the event that a prisoner escapes in another jurisdiction and is recaptured by that jurisdiction or by a South Salt Lake City police officer in that jurisdiction:
1. The local jurisdiction shall have priority in arresting and charging offenses against the prisoner.
 2. In the event that the local jurisdiction declines to process the prisoner or proceed with charges, the South Salt Lake City police officer shall take custody of the prisoner and proceed with the transport as before the escape.
 3. Charges for the escape may be added or screened with the appropriate prosecutor's office by the transporting officer.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Custodial Searches

906.4.8 TRANSPORT OF SICK, INJURED AND/OR DISABLED PRISONER

- (a) A disabled prisoner who requires the use of a wheelchair may be transported in a police vehicle as long as the officer is satisfied that it can be done safely, for both the officer and the prisoner.
 - 1. Wheelchairs, crutches, some prosthetic devices, etc., should be transported in the trunk of the transporting vehicle and not in a compartment of the vehicle where the prisoner has access.
- (b) Prisoners with prosthetic devices may be transported in a police vehicle.
 - 1. Restraining prisoners wearing prosthetic devices frequently requires ingenuity and concern for the safety of both the prisoner and the officer.
 - 2. A prisoner wearing a prosthetic device must be thoroughly searched, including the prosthetic device(s).
 - 3. Handcuffs and/or the leg cord cuff restraint (hobble) may be used to restrain prisoners wearing prosthetic device(s).
 - 4. Whatever restraining device or combination thereof is utilized should not interfere with the prisoner's ability to balance or protect him/herself during transport.
- (c) Prior to transporting a physically and/or mentally disabled prisoner or a prisoner wearing a prosthetic device(s) to a custodial facility, the transporting officer should contact the facility and advise them of the prisoner's condition so that any special arrangements may be made at the facility prior to the prisoner's arrival.
- (d) If a prisoner is so physically and/or mentally disabled that the officer feels the prisoner cannot be safely transported in a police vehicle, the officer shall contact the on-duty supervisor.
 - 1. The prisoner will, if possible, be processed and released in the field if a full booking procedure is not absolutely necessary.
 - 2. The prisoner may be transported to a booking or holding facility by ambulance. Any prisoner in custody for a criminal offense must be accompanied by an officer during transport in an ambulance.
- (e) Any prisoner complaining of sickness or injury, or who in the judgment of the officer appears to be sick or injured, whether complaining of same or not, will be treated as follows:
 - 1. A fire department aid unit will be called to the prisoner's location. Based upon the aid unit member's recommendation, the prisoner will be:
 - (a) Administered first aid by the aid crew.
 - (b) If medically indicated, transported to a department-approved emergency medical facility.
 - 1. The sick injured prisoner will likely be transported to a medical care facility by ambulance.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Custodial Searches

2. If, in the opinion of the aid crew members, the prisoner can be safely transported in a police vehicle in restraints, the police vehicle may be used for transport.
 3. If the prisoner has insurance providing medical care at a local medical care facility, he/she may be treated at that facility if he/she requests and it is practical to do so.
 4. Any prisoner in custody for a criminal offense must be accompanied by an officer during transport in an ambulance.
 5. If ambulance transportation to a medical facility is provided by ambulance for a person not under arrest, the officer will use his/her discretion on whether to accompany the prisoner in the ambulance or follow the ambulance in his/her patrol vehicle.
- (f) A written report will be made regarding any medical attention or first aid provided to a prisoner. The report shall include the dates, times, places, and names and/or identification numbers of the provider(s). The report will be filed with the case report. A copy of the aid unit report should be included in the case.
- (g) If a prisoner requires hospitalization, or dies in custody, command level personnel will be notified immediately.
- (h) Any medications belonging to a prisoner will be kept with the prisoner's property.
1. No member of this department will administer medication of any kind to any prisoner.

906.4.9 CONTROL OF PRISONERS TRANSPORTED TO MEDICAL FACILITIES

- (a) An officer will accompany any person who is under arrest and is transported to or from a medical care facility for treatment.
1. If the person being transported is not under arrest, the officer may follow the ambulance or medical aid unit to the medical facility.
- (b) Prisoners will remain restrained unless treatment dictates that the restraints are removed.
1. If restraints are removed the officer must exercise extreme caution to prevent the prisoner from causing undue harm to medical care providers, the officer, and/or him/herself.
 2. An officer should evaluate a suspects security risk based on criminal background, the nature of the offense, physical condition, and statements and actions observed.
 3. The officer will maintain visual contact with the prisoner as much as realistically possible, and will always maintain good security practices.
- (c) Anyone who is in-custody on South Salt Lake City criminal charges who, due to illness or injury are being housed as an in-patient in a medical care facility, will be the responsibility of this department.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Custodial Searches

1. If the prisoner is a security risk, it may be necessary for an officer to be posted outside of the prisoner's room to maintain the custody and security of the prisoner.
 - (a) This will be done at the request of the shift supervisor, who will notify the on-call commander at the earliest opportunity.
 - (b) Suspects under arrest for violent felony(s) will require an officer to be posted outside of the prisoner's room.
 - (c) Only the Chief of Police or his/her designee may make an exception to this section of the policy.
 - (d) All officers who are in charge of an in-patient prisoner will be rotated at regular intervals to prevent boredom and/or carelessness.
 - (e) Officers will also inspect any health care personnel allowed to enter the room, all food trays for utensils that may be used as weapons, and prohibit any personal contact by the prisoner, including telephone contact.
 2. If the prisoner does not pose a security risk, arrangements can be made with the medical facility to notify this agency when he/she is ready for discharge, and an officer can be dispatched at that time to take the prisoner into custody.
- (d) When a prisoner is released from a medical facility, whether in-patient or not, the officer should carefully record the prisoner's condition, treatment, and medication received.
 - (a) Ideally, an attending physician should provide this information in writing with his/her signature.
 - (e) Before transporting the prisoner, the officer search the prisoner again for weapons and/or contraband and properly restrain him/her in the vehicle.

906.5 PHYSICAL BODY CAVITY SEARCH

Physical body cavity searches shall be subject to the following (Utah Code 77-7-17.5):

- (a) No individual shall be subjected to a physical body cavity search without written approval of the Watch Commander and only upon a search warrant or approval of legal counsel. A copy of any search warrant and the results of the physical body cavity search shall be included with the related reports and made available, upon request, to the individual or authorized representative (except for those portions of the warrant ordered sealed by a court).
- (b) Only a physician may conduct a physical body cavity search.
- (c) Except for the physician conducting the search, persons present must be of the same sex as the individual being searched. Only the necessary [department/office] members needed to maintain the safety and security of the medical personnel shall be present.
- (d) Privacy requirements, including restricted touching of body parts and sanitary condition requirements, are the same as required for a strip search.
- (e) All such searches shall be documented, including (Utah Code 77-7-17.5):

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Custodial Searches

1. The facts that led to the decision to perform a physical body cavity search of the individual.
 2. The reasons less intrusive methods of searching were not used or were insufficient.
 3. The Watch Commander's approval.
 4. A copy of the search warrant.
 5. The time, date, and location of the search.
 6. The medical personnel present.
 7. The names, sex, and roles of any [department/office] members present.
 8. Any contraband or weapons discovered by the search.
 9. The procedures followed in performing the search and a description of the body areas searched.
- (f) A copy of the written authorization shall be retained and made available to the individual who was searched or other authorized representative upon request.

906.6 GENDER IDENTITY OR EXPRESSION CONSIDERATIONS

If an individual who is subject to a strip search or physical body cavity search has a gender identity or expression that differs from their sex assigned at birth, the search should be conducted by members of the same gender identity or expression as the individual, unless the individual requests otherwise.

906.7 JUVENILES

No juvenile should be subjected to a strip search or a physical body cavity search at the [Department/Office].

The Chief of Police or the authorized designee should establish procedures for the following:

- (a) Safely transporting a juvenile who is suspected of concealing a weapon or contraband, or who may be experiencing a medical issue related to such concealment, to a medical facility or juvenile detention facility as appropriate in the given circumstances.
 1. Procedures should include keeping a juvenile suspected of concealing a weapon under constant and direct supervision until custody is transferred to the receiving facility.
- (b) Providing officers with information identifying appropriate medical and juvenile detention facilities to which a juvenile should be transported for a strip or body cavity search.

Nothing in this section is intended to prevent an officer from rendering medical aid to a juvenile in emergency circumstances (see the Medical Aid and Response Policy for additional guidance).

906.8 TRAINING

The Training Sergeant shall ensure members have training that includes (28 CFR 115.115):

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Custodial Searches

- (a) Conducting searches of cross-gender individuals.
- (b) Conducting searches of transgender and intersex individuals.
- (c) Conducting searches in a professional and respectful manner, and in the least intrusive manner possible, consistent with security needs.

Prison Rape Elimination

907.1 PURPOSE AND SCOPE

This policy provides guidance for complying with the Prison Rape Elimination Act of 2003 (PREA) and the implementing regulation that establishes standards (PREA Rule) to prevent, detect and respond to sexual abuse, harassment and retaliation against prisoners in the South Salt Lake Police Department Temporary Holding Facilities (28 CFR 115.111).

907.1.1 DEFINITIONS

Definitions related to this policy include:

Intersex - A person whose sexual or reproductive anatomy or chromosomal pattern does not seem to fit typical definitions of male or female. Intersex medical conditions are sometimes referred to as disorders of sex development (28 CFR 115.5).

Sexual abuse - Any of the following acts, if the prisoner does not consent, is coerced into such act by overt or implied threats of violence or is unable to consent or refuse:

- Contact between the penis and the vulva or the penis and the anus, including penetration, however slight
- Contact between the mouth and the penis, vulva or anus
- Penetration of the anal or genital opening of another person, however slight, by a hand, finger, object or other instrument
- Any other intentional touching, either directly or through the clothing, of the genitalia, anus, groin, breast, inner thigh or the buttocks of another person, excluding contact incidental to a physical altercation (28 CFR 115.6)

Sexual abuse also includes abuse by a staff member, contractor or volunteer as follows, with or without consent of the prisoner or resident:

- Contact between the penis and the vulva or the penis and the anus, including penetration, however slight
- Contact between the mouth and the penis, vulva or anus
- Contact between the mouth and any body part where the staff member, contractor or volunteer has the intent to abuse, arouse or gratify sexual desire
- Penetration of the anal or genital opening, however slight, by a hand, finger, object or other instrument, that is unrelated to official duties, or where the staff member, contractor or volunteer has the intent to abuse, arouse or gratify sexual desire
- Any other intentional contact, either directly or through the clothing, of or with the genitalia, anus, groin, breast, inner thigh or the buttocks, that is unrelated to official duties, or where the staff member, contractor or volunteer has the intent to abuse, arouse or gratify sexual desire

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Prison Rape Elimination

- Any attempt, threat or request by a staff member, contractor or volunteer to engage in the activities described above
- Any display by a staff member, contractor or volunteer of his/her uncovered genitalia, buttocks or breast in the presence of a prisoner or resident
- Voyeurism by a staff member, contractor or volunteer (28 CFR 115.6)

Sexual harassment - Repeated and unwelcome sexual advances; requests for sexual favors; verbal comments, gestures or actions of a derogatory or offensive sexual nature by one prisoner or resident that are directed toward another; repeated verbal comments or gestures of a sexual nature to a prisoner or resident by a staff member, contractor or volunteer, including demeaning references to gender, sexually suggestive or derogatory comments about body or clothing, or obscene language or gestures (28 CFR 115.6).

Transgender - A person whose gender identity (i.e., internal sense of feeling male or female) is different from the person's assigned sex at birth (28 CFR 115.5).

907.2 POLICY

The South Salt Lake Police Department has zero tolerance toward all forms of sexual abuse and sexual harassment (28 CFR 115.111). The Department will not tolerate retaliation against any person who reports sexual abuse or sexual harassment or who cooperates with a sexual abuse or sexual harassment investigation.

The South Salt Lake Police Department will take immediate action to protect prisoners who are reasonably believed to be subject to a substantial risk of imminent sexual abuse (28 CFR 115.162).

907.3 PREA COORDINATOR

The Chief of Police shall appoint an upper-level manager with sufficient time and authority to develop, implement and oversee department efforts to comply with PREA standards in the South Salt Lake Police Department Temporary Holding Facilities (28 CFR 115.111). The PREA Coordinator's responsibilities shall include:

- (a) Developing and maintaining procedures to comply with the PREA Rule.
- (b) Ensuring that any contract for the confinement of South Salt Lake Police Department prisoners includes the requirement to adopt and comply with applicable PREA and the PREA Rule, including the obligation to provide incident-based and aggregated data, as required in 28 CFR 115.187 (28 CFR 115.112).
- (c) Developing a staffing plan to provide adequate levels of staffing and video monitoring, where applicable, in order to protect prisoners from sexual abuse (28 CFR 115.113). This includes documenting deviations and the reasons for deviations from the staffing plan, as well as reviewing the staffing plan a minimum of once per year.
- (d) Developing methods for staff to privately report sexual abuse and sexual harassment of prisoners (28 CFR 115.151).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Prison Rape Elimination

- (e) Developing a written plan to coordinate response among staff first responders, medical and mental health practitioners, investigators and department leadership to an incident of sexual abuse (28 CFR 115.165).
- (f) Ensuring a protocol is developed for investigating allegations of sexual abuse in the Temporary Holding Facility. The protocol shall include (28 CFR 115.121; 28 CFR 115.122):
 - 1. Evidence collection practices that maximize the potential for obtaining usable physical evidence based on the most recent edition of the U.S. Department of Justice's (DOJ) Office on Violence Against Women publication, "A National Protocol for Sexual Assault Medical Forensic Examinations, Adults/Adolescents" or a similarly comprehensive and authoritative protocol.
 - 2. A process to ensure a criminal or administrative investigation is completed on all allegations of sexual abuse or sexual harassment.
 - 3. A process to document all referrals to other law enforcement agencies.
 - 4. Access to forensic medical examinations, without financial cost, for all victims of sexual abuse where appropriate. Such examinations shall be performed by Sexual Assault Forensic Examiners (SAFEs) or Sexual Assault Nurse Examiners (SANEs) where possible. If SAFEs or SANEs cannot be made available, the examination can be performed by other qualified medical practitioners. The efforts to provide SAFEs or SANEs shall be documented.
 - 5. In accordance with security needs, provisions to permit, to the extent available, prisoner access to victim advocacy services if the prisoner is transported for a forensic examination to an outside hospital that offers such services.
- (g) Ensuring that prisoners with limited English proficiency and disabilities have an equal opportunity to understand and benefit from efforts to prevent, detect and respond to sexual abuse and sexual harassment. This includes, as appropriate, access to interpreters and written materials in formats or through methods that provide effective communication to those with disabilities (e.g., limited reading skills, intellectual, hearing or vision disabilities) (28 CFR 115.116).
 - 1. The agency shall not rely on other prisoners for assistance except in limited circumstances where an extended delay in obtaining an interpreter could compromise the prisoner's safety, the performance of first-response duties under this policy, or the investigation of a prisoner's allegations of sexual abuse, harassment or retaliation.
- (h) Publishing on the department's website:
 - 1. Information on how to report sexual abuse and sexual harassment on behalf of a prisoner (28 CFR 115.154).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Prison Rape Elimination

2. A protocol describing the responsibilities of the Department and any other investigating agency that will be responsible for conducting sexual abuse or sexual harassment investigations (28 CFR 115.122).
- (i) Establishing a process that includes the use of a standardized form and set of definitions to ensure accurate, uniform data is collected for every allegation of sexual abuse at facilities under this agency's direct control (28 CFR 115.187).
 1. The data collected shall include, at a minimum, the data necessary to answer all questions from the most recent version of the Survey of Sexual Violence, conducted by DOJ, or any subsequent form developed by DOJ and designated for lockups.
 2. The data shall be aggregated at least annually.
- (j) Ensuring audits are conducted pursuant to 28 CFR 115.401 through 28 CFR 115.405 for all Temporary Holding Facilities used to house prisoners overnight (28 CFR 115.193).
- (k) Ensuring contractors or others who work in the Temporary Holding Facility are informed of the agency's zero-tolerance policy regarding sexual abuse and sexual harassment (28 CFR 115.132).

907.4 REPORTING SEXUAL ABUSE AND HARASSMENT

Prisoners may make reports verbally, in writing, privately or anonymously of any of the following (28 CFR 115.151):

- Sexual abuse
- Sexual harassment
- Retaliation by other prisoners or staff for reporting sexual abuse or sexual harassment
- Staff neglect or violation of responsibilities that may have contributed to sexual abuse or sexual harassment

During intake the Department shall notify all prisoners of the zero-tolerance policy regarding sexual abuse and sexual harassment, and of at least one way to report abuse or harassment to a public or private entity that is not part of the Department and that is able to receive and immediately forward prisoner reports of sexual abuse and sexual harassment to agency officials. This allows the prisoner to remain anonymous (28 CFR 115.132; 28 CFR 115.151).

907.4.1 MEMBER RESPONSIBILITIES

Department members shall accept reports from prisoners and third parties and shall promptly document all reports (28 CFR 115.151).

All members shall report immediately to the Watch Commander any knowledge, suspicion or information regarding:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Prison Rape Elimination

- (a) An incident of sexual abuse or sexual harassment that occurs in the Temporary Holding Facility.
- (b) Retaliation against prisoners or the member who reports any such incident.
- (c) Any neglect or violation of responsibilities on the part of any department member that may have contributed to an incident or retaliation (28 CFR 115.161).

No member shall reveal any information related to a sexual abuse report to anyone other than to the extent necessary to make treatment and investigation decisions.

907.4.2 WATCH COMMANDER RESPONSIBILITIES

The Watch Commander shall report to the department's designated investigators all allegations of sexual abuse, harassment, retaliation, neglect or violations leading to sexual abuse, harassment or retaliation. This includes third-party and anonymous reports (28 CFR 115.161).

If the alleged victim is under the age of 18 or considered a vulnerable adult, the Watch Commander shall also report the allegation as required under mandatory reporting laws and department policy.

Upon receiving an allegation that a prisoner was sexually abused while confined at another facility, the Watch Commander shall notify the head of the facility or the appropriate office of the agency where the alleged abuse occurred. The notification shall be made as soon as possible but no later than 72 hours after receiving the allegation. The Watch Commander shall document such notification (28 CFR 115.163).

If an alleged prisoner victim is transferred from the Temporary Holding Facility to a jail, prison or medical facility, the Department shall, as permitted by law, inform the receiving facility of the incident and the prisoner's potential need for medical or social services, unless the prisoner requests otherwise (28 CFR 115.165).

907.5 INVESTIGATIONS

The Department shall promptly, thoroughly and objectively investigate all allegations, including third-party and anonymous reports, of sexual abuse or sexual harassment. Only investigators who have received department-approved special training shall conduct sexual abuse investigations (28 CFR 115.171).

907.5.1 FIRST RESPONDERS

The first officer to respond to a report of sexual abuse or sexual assault shall (28 CFR 115.164):

- (a) Separate the parties.
- (b) Establish a crime scene to preserve and protect any evidence. Identify and secure witnesses until steps can be taken to collect any evidence.
- (c) If the abuse occurred within a time period that still allows for the collection of physical evidence, request that the alleged victim not take any actions that could destroy physical evidence, including, as appropriate, washing, brushing teeth, changing clothes, urinating, defecating, smoking, drinking or eating.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Prison Rape Elimination

- (d) If the abuse occurred within a time period that still allows for the collection of physical evidence, ensure that the alleged abuser does not take any actions that could destroy physical evidence, including, as appropriate, washing, brushing teeth, changing clothes, urinating, defecating, smoking, drinking or eating.

If the first responder is not an officer the responder shall request that the alleged victim not take any actions that could destroy physical evidence and should then notify a law enforcement staff member (28 CFR 115.164).

907.5.2 INVESTIGATOR RESPONSIBILITIES

Investigators shall (28 CFR 115.171):

- (a) Gather and preserve direct and circumstantial evidence, including any available physical and biological evidence and any available electronic monitoring data.
- (b) Interview alleged victims, suspects and witnesses.
- (c) Review any prior complaints and reports of sexual abuse involving the suspect.
- (d) Conduct compelled interviews only after consulting with prosecutors as to whether compelled interviews may be an obstacle for subsequent criminal prosecution.
- (e) Assess the credibility of the alleged victim, suspect or witness on an individual basis and not by the person's status as a prisoner or a member of the South Salt Lake Police Department.
- (f) Document in written reports a description of physical, testimonial, documentary and other evidence, the reasoning behind any credibility assessments, and investigative facts and findings.
- (g) Refer allegations of conduct that may be criminal to the prosecutor's office for possible prosecution, including any time there is probable cause to believe a prisoner sexually abused another prisoner in the Temporary Holding Facility (28 CFR 115.178).
- (h) Cooperate with outside investigators and remain informed about the progress of any outside investigation.

907.5.3 ADMINISTRATIVE INVESTIGATIONS

Administrative investigations shall include an effort to determine whether staff actions or failures to act contributed to the abuse. The departure of the alleged abuser or victim from the employment or control of this department shall not be used as a basis for terminating an investigation (28 CFR 115.171).

907.5.4 SEXUAL ASSAULT AND ABUSE VICTIMS

No prisoner who alleges sexual abuse shall be required to submit to a polygraph examination or other truth-telling device as a condition for proceeding with the investigation of such an allegation (28 CFR 115.171(e)).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Prison Rape Elimination

Prisoner victims of sexual abuse shall receive timely, unimpeded access to emergency medical treatment. Treatment services shall be provided to the victim without financial cost and regardless of whether the victim names the abuser or cooperates with any investigation arising out of the incident (28 CFR 115.182).

907.5.5 CONCLUSIONS AND FINDINGS

All completed investigations shall be forwarded to the Chief of Police, or if the allegations may reasonably involve the Chief of Police, to the Mayor. The Chief of Police or Mayor shall review the investigation and determine whether any allegations of sexual abuse or sexual harassment have been substantiated by a preponderance of the evidence (28 CFR 115.172).

All personnel shall be subject to disciplinary sanctions up to and including termination for violating this policy. Termination shall be the presumptive disciplinary sanction for department members who have engaged in sexual abuse. All discipline shall be commensurate with the nature and circumstances of the acts committed, the member's disciplinary history and the sanctions imposed for comparable offenses by other members with similar histories (28 CFR 115.176).

All terminations for violations of this policy, or resignations by members who would have been terminated if not for their resignation, shall be criminally investigated unless the activity was clearly not criminal and reported to any relevant licensing body (28 CFR 115.176).

Any contractor or volunteer who engages in sexual abuse shall be prohibited from contact with prisoners and reported to any relevant licensing bodies (28 CFR 115.177). The Chief of Police shall take appropriate remedial measures and consider whether to prohibit further contact with prisoners by a contractor or volunteer.

907.6 RETALIATION PROHIBITED

All prisoners and members who report sexual abuse or sexual harassment or who cooperate with sexual abuse or sexual harassment investigations shall be protected from retaliation (28 CFR 115.167). If any other individual who cooperates with an investigation expresses a fear of retaliation, appropriate measures shall be taken to protect that individual.

The Watch Commander or the authorized designee shall employ multiple protection measures, such as housing changes or transfers for prisoner victims or abusers, removal of alleged abusers from contact with victims, and emotional support services for prisoners or members who fear retaliation for reporting sexual abuse or sexual harassment or for cooperating with investigations.

The Watch Commander or the authorized designee shall identify a staff member to monitor the conduct and treatment of prisoners or members who have reported sexual abuse and of prisoners who were reported to have suffered sexual abuse. The staff member shall act promptly to remedy any such retaliation. In the case of prisoners, such monitoring shall also include periodic status checks.

907.7 REVIEWS AND AUDITS

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Prison Rape Elimination

907.7.1 INCIDENT REVIEWS

An incident review shall be conducted at the conclusion of every sexual abuse investigation, unless the allegation has been determined to be unfounded. The review should occur within 30 days of the conclusion of the investigation. The review team shall include upper-level management officials and seek input from line supervisors and investigators (28 CFR 115.186).

The review shall (28 CFR 115.186):

- (a) Consider whether the allegation or investigation indicates a need to change policy or practice to better prevent, detect or respond to sexual abuse.
- (b) Consider whether the incident or allegation was motivated by race; ethnicity; gender identity; lesbian, gay, bisexual, transgender or intersex identification, status or perceived status; gang affiliation; or was motivated or otherwise caused by other group dynamics at the facility.
- (c) Examine the area in the facility where the incident allegedly occurred to assess whether physical barriers in the area may enable abuse.
- (d) Assess the adequacy of staffing levels in that area during different shifts.
- (e) Assess whether monitoring technology should be deployed or augmented to supplement supervision by staff.

The review team shall prepare a report of its findings, including any determinations made pursuant to this section and any recommendations for improvement. The report shall be submitted to the Chief of Police and the PREA Coordinator. The Chief of Police or the authorized designee shall implement the recommendations for improvement or shall document the reasons for not doing so (28 CFR 115.186).

907.7.2 DATA REVIEWS

The facility shall conduct an annual review of collected and aggregated incident-based sexual abuse data. The review should include, as needed, data from incident-based documents, including reports, investigation files and sexual abuse incident reviews (28 CFR 115.187).

The purpose of these reviews is to assess and improve the effectiveness of sexual abuse prevention, detection and response policies, practices and training. An annual report shall be prepared that includes (28 CFR 115.188):

- (a) Identification of any potential problem areas.
- (b) Identification of any corrective actions taken.
- (c) Recommendations for any additional corrective actions.
- (d) A comparison of the current year's data and corrective actions with those from prior years.
- (e) An assessment of the department's progress in addressing sexual abuse.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Prison Rape Elimination

The report shall be approved by the Chief of Police and made readily available to the public through the department website or, if it does not have one, through other means. Material may be redacted from the reports when publication would present a clear and specific threat to the safety and security of the Temporary Holding Facility. However, the nature of the redacted material shall be indicated.

All aggregated sexual abuse data from South Salt Lake Police Department facilities and private facilities with which it contracts shall be made readily available to the public at least annually through the department website or, if it does not have one, through other means. Before making aggregated sexual abuse data publicly available, all personal identifiers shall be removed (28 CFR 115.189).

907.8 RECORDS

The Department shall retain all written reports from administrative and criminal investigations pursuant to this policy for as long as the alleged abuser is held or employed by the Department, plus five years (28 CFR 115.171).

All other data collected pursuant to this policy shall be securely retained for at least 10 years after the date of the initial collection unless federal, state or local law requires otherwise (28 CFR 115.189).

907.9 TRAINING

All employees, volunteers and contractors who may have contact with prisoners shall receive department-approved training on the prevention and detection of sexual abuse and sexual harassment within this facility. The Training Coordinator shall be responsible for developing and administering this training as appropriate, covering at a minimum (28 CFR 115.131):

- The Department's zero-tolerance policy and prisoners' right to be free from sexual abuse and sexual harassment, and from retaliation for reporting sexual abuse or harassment.
- The dynamics of sexual abuse and harassment in confinement settings, including which prisoners are most vulnerable.
- The right of prisoners and staff members to be free from sexual abuse and sexual harassment, and from retaliation for reporting sexual abuse or harassment.
- Detecting and responding to signs of threatened and actual abuse.
- Communicating effectively and professionally with all prisoners.
- Compliance with relevant laws related to mandatory reporting of sexual abuse to outside authorities.

Investigators assigned to sexual abuse investigations shall also receive training in conducting such investigations in confinement settings. Training should include (28 CFR 115.134):

- Techniques for interviewing sexual abuse victims.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Prison Rape Elimination

- Proper use of *Miranda* and *Garrity* warnings.
- Sexual abuse evidence collection in confinement settings.
- Criteria and evidence required to substantiate a case for administrative action or prosecution referral.

The Training Coordinator shall maintain documentation that employees, volunteers, contractors and investigators have completed required training and that they understand the training. This understanding shall be documented through individual signature or electronic verification.

Transporting Persons in Custody

908.1 PURPOSE AND SCOPE

This policy provides guidelines for transporting persons who are in the custody of the South Salt Lake Police Department.

See the Handcuffing and Restraints Policy for additional guidance.

908.2 POLICY

It is the policy of the South Salt Lake Police Department to provide safe, secure, and humane transportation for all persons in custody.

908.3 PATROL DIVISION COMMANDER RESPONSIBILITIES

The Patrol Division Commander should establish related procedures for:

- Safely transporting persons who have their legs restrained.
- Seating placement of persons being transported in vehicles with and without safety barriers.

908.4 OFFICER RESPONSIBILITIES

Persons in custody should be transported in a vehicle properly equipped to transport passengers. They should be appropriately restrained and positioned during transport.

Officers transporting a person in custody should:

- (a) Search all areas of the vehicle accessible to a person in custody before and after each transport.
- (b) Immediately search persons in custody after arrest, when receiving the person from the custody of another officer, and before transferring the person. Refer to the Custodial Searches Policy before conducting any search other than a field search.
 1. Whenever practicable, a search should be conducted by an officer of the same gender as the person being searched. If an officer of the same gender is not reasonably available, a witnessing officer should be present during the search.
- (c) Provide Dispatch with any required notifications (e.g., start time, mileage, end time).
- (d) Properly secure all property.
- (e) Use audio/video equipment (when properly equipped) to observe and record any person in custody during transport (see the Mobile Audio/Video and Body-Worn Cameras policies for additional guidance).
- (f) Make a reasonable effort to prevent inappropriate conversations between persons being transported (e.g., demeaning or insulting language) or conversations between a person being transported and someone outside the vehicle.
- (g) Plan travel times and routes to avoid situations that might impede transportation (e.g., heavy traffic, unfavorable road conditions, extreme weather) when reasonably practicable.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Transporting Persons in Custody

- (h) Make a verbal welfare check with a person in custody at least every 10 minutes. Provide sufficient visual observation and audio communication during the transport of:
 - 1. Individuals in auxiliary restraints.
 - 2. Individuals in leg restraints.
 - 3. Individuals wearing a spit hood.
 - 4. Individuals who are a suspected suicide risk.
- (i) Verify that the vehicle's security devices (e.g., window and rear-door child-safety locks) are activated.
- (j) Assess uncooperative persons who cannot or will not sit upright for a medical condition (see the Medical Aid and Response Policy for additional guidance):
 - 1. If no medical condition exists, alternative transportation should be arranged (e.g., a special transport van).

908.5 TRANSPORT RESTRICTIONS

When transporting multiple persons, officers:

- (a) Should not transport persons in custody together. Persons in custody should be transported individually when practicable, or within their own compartment of a multiple-compartment vehicle, unless supervisor approval is received based on unusual circumstances.
 - 1. Juveniles and adults shall not be transported together.
 - 2. Persons with known hostilities toward each other, such as mutual combatants or rival gang members, shall not be transported together.
 - 3. Persons of different genders should not be transported together.
- (b) If segregating individuals is not possible, transporting officers should be alert to inappropriate physical or verbal contact and take appropriate action.

908.6 TRANSPORT VANS

An officer trained on the safety and restraint systems of a transport van should be present during the transport van's use for transporting a person in custody.

An officer should assist persons getting into and out of the transport van to avoid falls.

908.7 TRANSPORTING PERSONS IN CUSTODY WHO HAVE A DISABILITY

When transporting a person in custody who has a disability, a transporting officer should request assistance as necessary to transport the person in a reasonable and safe manner. The transporting officer should ensure that any special equipment (e.g., canes, wheelchairs, prosthetics) is transported to the person's destination in a way that does not threaten the safety or security of the person in custody or the officer.

Officers transporting a person who has a disability should consult with the person in custody and use good judgment in determining what, if any, restraining devices may be appropriate based on the person's disability to ensure the security, safety, and dignity of all persons.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Transporting Persons in Custody

908.8 TRANSPORTING ILL OR INJURED PERSONS IN CUSTODY

Except in exceptional cases where alternatives are not reasonably available, officers should not transport persons in custody who are unconscious, have serious injuries, or who may be seriously ill. EMS personnel should be called to handle such transportation.

Officers shall notify a supervisor as soon as practicable when transporting a person in custody to a hospital.

An officer should accompany any person in custody during transport in an ambulance when requested by EMS personnel, when it reasonably appears necessary to provide security, when it is necessary for investigative purposes, or when so directed by a Watch Commander.

Any person in custody suspected of having a communicable disease should be transported in compliance with the exposure control plan in the Communicable Diseases Policy.

See the Medical Aid and Response Policy for additional guidance on ill or injured persons in custody.

908.9 TRANSPORTING PREGNANT PERSONS IN CUSTODY

Persons in custody who are known to be pregnant should be restrained during transport in the least restrictive manner that is effective for officer safety. Leg restraints, waist chains, or handcuffs behind the body should not be used unless the officer has a reasonable suspicion that the person may resist, attempt escape, injure themselves or others, or damage property.

Absent exceptional circumstances, persons in labor or delivery should not be transported by officers. EMS personnel should be called to handle transportation.

908.10 INVOLUNTARY COMMITMENT TRANSPORTS

When transporting any individual for an involuntary commitment, the transporting officer should request that Dispatch notify the receiving facility of the estimated time of arrival, the level of cooperation of the individual, and whether any special medical care is needed.

See the Involuntary Commitments Policy for additional guidance.

908.11 INTERRUPTION OF TRANSPORT

Absent extraordinary circumstances, officers should not interrupt a transport to provide emergency assistance without supervisory approval. Officers encountering an emergency should notify Dispatch and request an appropriate response.

908.12 EXTENDED TRANSPORTS

During transports for extended durations, transporting officers may be required to make necessary stops. With supervisory approval and due consideration for security risks and the in-custody person's health and well-being, these stops should be limited to fuel, meals, bathroom breaks, and other purposes reasonably necessary for the continuation of the transport.

908.13 PROHIBITIONS

When transporting a person in custody, officers should not:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Transporting Persons in Custody

- (a) Use transport as a form of punishment or retaliation (e.g., intentionally rough rides, excessive heat or cold, obnoxiously loud music).
- (b) Handcuff a person to any part of a vehicle.
- (c) Leave the vehicle unattended with the person in custody in the vehicle.
- (d) Allow any person who is not in custody (e.g., friend, family member) to have contact with or be in close proximity to the person in custody.
- (e) Allow any food, drink, or other consumables to be given to the person in custody by anyone other than [department/office] personnel or receiving agency personnel.
- (f) Stop to conduct any personal activities.
- (g) Engage in a pursuit.

908.14 ESCAPES

In the event that a person in custody escapes while being transported, the transporting officer should immediately advise Dispatch and other units of the escape, provide a description of the escapee, notify the Watch Commander, and submit a written report as soon as practicable describing the circumstances of the escape and any recapture.

The Watch Commander should notify the Chief of Police or the authorized designee upon learning of an escape.

If the escape occurs outside the jurisdiction of the South Salt Lake Police Department, the Watch Commander should notify the appropriate agency or agencies within the jurisdiction where the escape occurred.

908.15 DOCUMENTATION

If a person is injured during transportation, officers should document the injury in the appropriate report. Documentation should include the condition of the person prior to transportation and the known or suspected causes of the injury during transportation (e.g., hitting head, struggling with restraints, fighting with other persons in custody). Any visible or reported injuries should be photographed and included with the report.

908.16 NOTIFICATIONS

Officers should notify a supervisor and any receiving facility of information regarding any circumstances the officer reasonably believes would be potential safety concerns or medical risks to the person (e.g., uncooperative or violent, prolonged struggle, extreme agitation, medical conditions) that may have occurred prior to, or during, transportation.

908.17 TRAINING

The Training Coordinator should provide periodic training on this policy and procedures related to transporting persons in custody, restraint systems, and restraint devices.

Chapter 10 - Personnel

RECRUITMENT, SELECTION and STANDARDS

1000.1 PURPOSE AND SCOPE

This policy provides a framework for employee recruiting efforts and identifying job-related standards for the selection process. This policy supplements the rules that govern employment practices for the South Salt Lake Police Department and that are promulgated and maintained by the Department of Human Resources.

1000.2 POLICY

In accordance with applicable federal, state, and local law, the South Salt Lake Police Department provides equal opportunities for applicants and employees regardless of actual or perceived race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, age, disability, pregnancy, genetic information, veteran status, marital status, and any other classification or status protected by law. The [Department/Office] does not show partiality or grant any special status to any applicant, employee, or group of employees unless otherwise required by law.

The [Department/Office] will recruit and hire only those individuals who demonstrate a commitment to service and who possess the traits and characteristics that reflect personal integrity and high ethical standards.

1000.3 RECRUITMENT

The Administration Division Commander shall employ a comprehensive recruitment and selection strategy to recruit and select employees from a qualified and diverse pool of candidates.

The strategy shall include:

- (a) Establishment of a written recruitment plan.
 - 1. The plan shall include an outline of steps for recruiting candidates who are representative of the community. This should include candidates who live in or are from the community. If appropriate and consistent with applicable laws and memorandums of understanding or collective bargaining agreements.
- (b) Identification of racially and culturally diverse target markets.
- (c) Use of marketing strategies to target diverse applicant pools.
- (d) Expanded use of technology and maintenance of a strong internet presence. This may include an interactive [department/office] website and the use of [department/office]-managed social networking sites, if resources permit.
- (e) Expanded outreach through partnerships with media, community groups, citizen academies, local colleges, universities, and the military.
- (f) Employee referral and recruitment incentive programs.
- (g) Consideration of shared or collaborative regional testing processes.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

RECRUITMENT, SELECTION and STANDARDS

The Administration Division Commander shall avoid advertising, recruiting, and screening practices that tend to stereotype, focus on homogeneous applicant pools, or screen applicants in a discriminatory manner.

The [Department/Office] should strive to facilitate and expedite the screening and testing process, and should periodically inform each candidate of their status in the recruiting process.

1000.4 SELECTION PROCESS

The [Department/Office] shall actively strive to identify a diverse group of candidates who have in some manner distinguished themselves as being outstanding prospects. Minimally, the [Department/Office] shall employ a comprehensive screening, background investigation, and selection process that assesses cognitive and physical abilities and includes review and verification of the following:

- (a) A comprehensive application for employment (including previous employment, references, current and prior addresses, education, military record)
- (b) Driving record
- (c) Personal and professional reference checks
- (d) Employment eligibility, including U.S. Citizenship and Immigration Services (USCIS) Employment Eligibility Verification Form I-9 and acceptable identity and employment authorization documents. This required documentation should not be requested until a candidate is hired. This does not prohibit obtaining documents required for other purposes.
- (e) Information obtained from public internet sites
 - 1. This review should include the identification of any activity that promotes or supports unlawful violence or unlawful bias against persons based on protected characteristics (e.g., race, ethnicity, national origin, religion, gender, gender identity, sexual orientation, disability).
- (f) Financial history consistent with the Fair Credit Reporting Act (FCRA) (15 USC § 1681 et seq.)
- (g) Local, state, and federal criminal history record checks
- (h)
- (i) Medical and psychological examination (may only be given after a conditional offer of employment)
- (j) Review board or selection committee assessment
- (k) Relevant national and state decertification records, if available
- (l) Any relevant information in the National Law Enforcement Accountability Database

1000.4.1 VETERAN AND SERVICE MEMBER PREFERENCE

The [Department/Office] will provide preference eligibility for veterans and service member applicants as required by Utah Code 71A-2-102.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

RECRUITMENT, SELECTION and STANDARDS

1000.5 BACKGROUND INVESTIGATION

Every candidate shall undergo a thorough background investigation to verify their personal integrity and high ethical standards, and to identify any past behavior that may be indicative of the candidate's unsuitability to perform duties relevant to the operation of the South Salt Lake Police Department (Utah Code 53-14-102).

In addition to the requirements of Utah Code 53-14-103, the background investigation shall include but not be limited to the following:

- (a) Verification of qualifying credentials
- (b) Criminal history report
- (c) Verification of personal and professional references
- (d) Education verification
- (e) Employment history verification
- (f) A review of relevant national or state decertification records, including the National Decertification Index operated by the International Association of Directors of Law Enforcement Standards and Training (IADLEST)
- (g) A review of the National Law Enforcement Accountability Database (NLEAD) (when made accessible to non-federal law enforcement agencies)
- (h) Consistent with the First Amendment and all applicable laws, a check of publicly available internet and information-sharing sites to identify activity that promotes or supports unlawful violence or unlawful bias against persons based on race, ethnicity, national origin, religion, gender, gender identity, sexual orientation, or disability

1000.5.1 NOTICES

Background investigators shall ensure that investigations are conducted and notices provided in accordance with the requirements of the FCRA (15 USC § 1681d).

1000.5.2 REVIEW OF SOCIAL MEDIA SITES

Due to the potential for accessing unsubstantiated, private, or protected information, the Administration Division Commander shall not require candidates to provide passwords, account information, or access to password-protected social media accounts (Utah Code 34-48-201).

The Administration Division Commander should consider utilizing the services of an appropriately trained and experienced third party to conduct open source, internet-based searches and/or review information from social media sites to ensure that:

- (a) The legal rights of candidates are protected.
- (b) Material and information to be considered are verified, accurate and validated.
- (c) The [Department/Office] fully complies with applicable privacy protections and local, state and federal law.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

RECRUITMENT, SELECTION and STANDARDS

Regardless of whether a third party is used, the Administration Division Commander should ensure that potentially impermissible information is not available to any person involved in the candidate selection process.

1000.5.3 DOCUMENTING AND REPORTING

The background investigator shall summarize the results of the background investigation in a report that includes sufficient information to allow the reviewing authority to decide whether to extend a conditional offer of employment. The report shall not include any information that is prohibited from use, including that from social media sites, in making employment decisions. The report and all supporting documentation shall be included in the candidate's background investigation file.

1000.5.4 RECORDS RETENTION

The background report and all supporting documentation shall be maintained in accordance with the established records retention schedule.

1000.6 DISQUALIFICATION GUIDELINES

As a general rule, performance indicators and candidate information and records shall be evaluated by considering the candidate as a whole, and taking into consideration the following:

- Age at the time the behavior occurred
- Passage of time
- Patterns of past behavior
- Severity of behavior
- Probable consequences if past behavior is repeated or made public
- Likelihood of recurrence
- Relevance of past behavior to public safety employment
- Aggravating and mitigating factors
- Other relevant considerations

A candidate's qualifications will be assessed on a case-by-case basis, using a totality-of-the-circumstances framework.

1000.7 EMPLOYMENT STANDARDS

All candidates shall meet the minimum standards required by state law (Utah Code 53-6-203; Utah Code 53-6-302). Candidates will be evaluated based on merit, ability, competence, and experience, in accordance with the high standards of integrity and ethics valued by the [Department/Office] and the community.

Validated, job-related, and nondiscriminatory employment standards shall be established for each job classification and shall minimally identify the training, abilities, knowledge, and skills required to perform the position's essential duties in a satisfactory manner. Each standard should include

South Salt Lake Police Department

South Salt Lake PD Policy Manual

RECRUITMENT, SELECTION and STANDARDS

performance indicators for candidate evaluation. The Department of Human Resources should maintain validated standards for all positions.

1000.7.1 STANDARDS FOR OFFICERS

Candidates shall meet the minimum standards established by the Utah Peace Officer Standards and Training (POST) Council (Utah Code 53-6-203):

- (a) Citizen of the United States, United States national, or lawful permanent resident who has legal authorization to work in the United States and has been in the United States legally for at least five years immediately preceding the day on which the application is made
- (b) At least 21 years old
- (c) High school graduate or possess an equivalent achievement
- (d) Not have been convicted of a crime for which the candidate could be punished by imprisonment
- (e) Demonstrate good moral character as determined through a background investigation. A candidate shall be considered to be of good moral character if they have not engaged in conduct that would violate Utah Code 53-6-211(1)
- (f) Be free of any physical, emotional, or mental condition that might adversely affect the performance of the candidate's duties as a peace officer
- (g) Criminal background check of local, state, and national criminal history files
- (h) Not prohibited from possessing a firearm under state or federal law
- (i) Meet all other standards required by POST

Before hiring a candidate who is working, or has previously worked, for another law enforcement agency, the Administration Division Commander shall comply with the verification and background check requirements of Utah Code 53-14-102.

In addition to the standards established by POST, the [Department/Office] may establish additional standards concerning peace officer candidates (Utah Code 53-6-207).

1000.8 PROBATIONARY PERIODS

The Administrative Division Commander should coordinate with the South Salt Lake Department of Human Resources to identify positions subject to probationary periods and procedures for:

- (a) Appraising performance during probation.
- (b) Assessing the level of performance required to complete probation.
- (c) Extending probation.
- (d) Documenting successful or unsuccessful completion of probation.
- (e) Once an officer completes their assigned field training they will be placed on an 12 month probationary period.

PROMOTIONS AND SPECIALTY ASSIGNMENTS

1001.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for promotions and for making special assignments within the South Salt Lake Police Department.

1001.2 POLICY

The South Salt Lake Police Department determines assignments and promotions in a non-discriminatory manner based upon job-related factors and candidate skills and qualifications. Assignments and promotions are made by the Chief of Police.

1001.3 DEPUTY CHIEF APPOINTMENT

A. Appointment Eligibility

(a) Internal and External Candidates:

- The appointment of Deputy Chief may be made from any sworn position within the South Salt Lake Police Department or from outside the department.

(b) Discretion of the Agency Head:

- The Chief of Police has the discretion to select the candidate for Deputy Chief, provided the candidate meets the minimum requirements as set forth in the Deputy Chief job description.

B. Minimum Requirements

(a) Certification:

- The candidate must be a certified peace officer/deputy in the State of Utah.

(b) Experience:

- The candidate must have law enforcement management experience.

C. Nature of Appointment

(a) At-Will Position:

- The Deputy Chief position is an at-will appointment.

(b) Return to Previous Rank:

- If the candidate is selected from within the ranks of the South Salt Lake Police Department, upon completion of the assignment or change in personnel, the individual will return to their previous rank prior to the appointment.

D. Appointment Process

(a) Announcement and Recruitment:

- The appointment process may begin with an internal or external announcement, detailing the minimum requirements and the process for application.

(b) Application Submission:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

PROMOTIONS AND SPECIALTY ASSIGNMENTS

- Interested candidates must submit their applications, which may include a resume, cover letter, and any other required documentation.
- (c) **Review and Selection:**
 - The Chief of Police will review applications and conduct interviews with qualified candidates.
 - The selection will be based on the candidate's qualifications, experience, and fit for the role.
- (d) **Final Decision:**
 - The Chief of Police makes the final decision on the appointment of the Deputy Chief.

E. Transition and Integration

- (a) **Orientation:**
 - An orientation program will be provided for the new Deputy Chief to ensure a smooth transition into the role.
- (b) **Mentorship:**
 - A mentorship arrangement may be established to support the new Deputy Chief during the initial period of their appointment.

1001.4 POLICE OFFICER II

- A. An officer that qualifies for the Police Officer II Promotional Career Enhancement must submit an application to the Office of the Chief of Police for review.
- B. The application process is the promotional process for Police Officer II.
- C. Written approval of promotion will be given to the officer from Human Resources Department.

1001.5 PROMOTIONAL PROCESS

A. Evaluation of Promotional Candidates

- (a) **The Chief of Police or designee will conducted testing and assessment for promotional opportunities in the following manner:**
 - **Job Task Analysis:** Conduct testing that measures dimensions, attributes, characteristics, qualities, skills, abilities, or knowledge specified in a written job task analysis.
 - **Multiple Assessors:** Utilize multiple assessors who have administrative experience and good standing in this department or another agency.
 - Assessors shall be instructed and briefed prior to participating in the process.
 - **Evaluation Techniques:** Employ techniques designed to provide information used in evaluating the dimensions, attributes, and/or qualities previously determined.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

PROMOTIONS AND SPECIALTY ASSIGNMENTS

- **Simulated Job-Related Exercises:** Use simulated job-related exercises that have been pre-tested to ensure they provide reliable, objective, and relevant information.
- **Documentation:** Maintain forms utilized to record and document the observations of assessors at each stage of the process.

B. Promotional Process Procedures

(a) **Notification of Promotional Opportunity:**

- Notify employees of promotional opportunities via email or other written notice.
- The notice will include minimum qualifications, dates, and times of any testing to be conducted.
- All candidates must be Crisis Intervention Team Training Currently Certified.
- All candidates must have obtained their POST Mid-Management Certification.
- Sergeant candidates must have a combined total of five years of law enforcement experience, with a minimum of three years as an officer with the South Salt Lake Police Department. Prior correction/jail/prison related service will be credited at two years of service equals for every one year of service for calculation purposes.
- Lieutenant candidates must have a combined total of five years of law enforcement experience with at least two years of supervisory experience. Prior correction/jail/prison related service will be credited at two years of services equals for every one year of service for calculation purposes.

(b) **Application Submission:**

- Each applicant shall submit resumes, cover letters, supporting required documents and/or letters of intent to the Office of the Chief, as outlined in the promotional email.
-

(c) **Testing Process:**

- May include written abilities testing, oral interviews, and/or presentation on a topic.
- Tests and oral questions will be specific to the vacant position.
- A minimum of five internal applicants is required to keep the process internal. If there is less than five applicants, the promotional process opportunity shall be listed externally.
- Four hours of straight comp time is authorized for the testing process. Overtime is not authorized.

(d) **Candidate Selection:**

- After the testing and assessment, the names of the top five (5) candidates will be submitted to the Chief of Police.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

PROMOTIONS AND SPECIALTY ASSIGNMENTS

- The Chief of Police may interview the candidates, review their personnel files and/or prior performance evaluations.
 - The Chief of Police will take the qualified list to the administrative team for input and review.
 - The selected candidate will be notified in writing of the promotion, if accepted the candidate will have to submit to a drug screen.
 - The candidate will be promoted at a date and time determined in coordination with the Human Resources Department and the City Recorder.
- (e) **Eligibility Pools:**
- (a) **Creation of Eligibility Pool:**
 - Promotional candidates who successfully complete the selection process will be placed on an eligibility pool list.
 - All candidates in the eligibility pool are ranked by score at this stage of the promotional process.
 - (b) **Validity Period:**
 - The eligibility pool is valid for twelve (12) months from the published date.
 - The Chief of Police has the discretion to vacate the eligibility pool prior to the end of the twelve (12) months.
 - (c) **Review and Certification:**
 - The Chief of Police will review the results, address any issues, and certify the pool in accordance with this policy.
 - (d) **Extension of Eligibility Pool:**
 - The Human Resources Department may extend the validity of the eligibility pool at the request of the Chief of Police or their designee.
- (f) **Final Selection:**
- The Chief of Police will make the final selection based on all elements in the promotional process and the needs of the department
 - **Notification of Promotion:**
 - (a) The Chief of Police or designee will notify the Human Resources Department of the candidate(s) selected for promotion.

C. Promotional Process Records

- (a) **Record Security and Access:**
- Secure records related to any promotional process in a file accessible only to individuals authorized by the Chief of Police or the Human Resources Department.
- (b) **Documentation Retention:**

South Salt Lake Police Department

South Salt Lake PD Policy Manual

PROMOTIONS AND SPECIALTY ASSIGNMENTS

- Ensure that all documentation related to the promotional process, including test results, assessment forms, and final selection records, are retained according to the department's records retention policy.

D. Best Practices for the Promotional Process

(a) **Transparency and Fairness:**

- Ensure the promotional process is transparent and fair, providing equal opportunities for all eligible employees.

(b) **Assessor Training:**

- Provide training and briefing for assessors to ensure they understand the process and criteria for evaluation.

(c) **Consistency in Testing:**

- Utilize standardized tests and simulated exercises that are consistent across all candidates to maintain objectivity.

(d) **Feedback Mechanism:**

- Offer feedback to candidates post-assessment to help them understand their performance and areas for improvement.

(e) **Continuous Improvement:**

- Regularly review and update the promotional process to incorporate best practices and address any identified issues

1001.5.1 PROMOTIONAL REVIEW AND APPEALS

- A. Any promotional candidate may review their own answer key and scores of the assessment promotional process, no sooner than five (5) days after the completion of the total process.
- B. Any employee contesting the promotional process or any element of the process, shall comply with the City grievance procedures.
- C. Any re-application, re-testing, or re-evaluation regarding an appeal of the promotional process is done solely at the discretion of the Chief of Police.

1001.6 PROMOTION PROBATIONARY PERIOD

- A. After an officer or professional support personnel has been approved or accepted a promotion, they will be in a probationary status for one year.

1001.7 SPECIAL ASSIGNMENT SELECTION

- A. Special assignments that are opened for general application shall be advertised by written [department/office]-wide announcement, and all qualified members will be allowed to apply and compete for positions.

1001.8 SPECIAL ASSIGNMENT POSITIONS

The following positions are considered special assignments and not promotions:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

PROMOTIONS AND SPECIALTY ASSIGNMENTS

- (a) Detective
- (b) Motor officer
- (c) Bicycle Patrol officer
- (d) Canine handler
- (e) Collision investigator
- (f) Homeless Resource Officer
- (g) Field Training Officer
- (h) Community Resource Officer; Neighborhood Watch, Business Watch
- (i) School Resource Officer
- (j) Youth Resource officer
- (k) Child Abduction Response Team
- (l) SWAT
- (m) Crisis Negotiator
- (n) Department Training Officer
- (o) Public Order Assigned Officer
- (p) UAS Operator
- (q) Major Accident Officer

1001.8.1 GENERAL REQUIREMENTS

The following requirements should be considered when selecting a candidate for a special assignment:

The candidate must:

- (a) Have completed probation or wavier from the Chief of Police
- (b) Possessor be able to obtain any certification required by POST or law
- (c) Possess exceptional skills, experience, or abilities related to the special assignment

1001.8.2 EVALUATION CRITERIA

The following criteria will be used in evaluating candidates for a special assignment:

- (a) Presents a professional, neat appearance.
- (b) Maintains a physical condition that aids in the candidate's performance.
- (c) Expressed an interest in the assignment.
- (d) Demonstrates the following traits:
 - 1. Emotional stability and maturity
 - 2. Stress tolerance
 - 3. Sound judgment and decision-making

South Salt Lake Police Department

South Salt Lake PD Policy Manual

PROMOTIONS AND SPECIALTY ASSIGNMENTS

4. Personal integrity and ethical conduct
5. Leadership skills
6. Initiative
7. Adaptability and flexibility
8. Ability to conform to [department/office] goals and objectives in a positive manner

1001.8.3 SELECTION PROCESS

The selection process for special assignments will include an administrative evaluation as determined by the Chief of Police to include:

- a. Review of resume, cover letter and any additional supporting documentation (Letter of reference or recommend, specific training or skills)
- b. Review of personnel file to ensure the applicant is in good standing.
- c. An interview process may be elected, if needed. The interview panel will consist of a minimum of three evaluators.
- d. Final packets will be presented for an administrative review. The administrative review will be assessed by a minimum of two lieutenants, with input from the deputy chief.
- e. The Chief of Police will review the recommended applicants and make the final decision on the selected applicant.
- f. The selection process for all special assignment positions may be waived for temporary assignments, emergency situations, training, and at the discretion of the Chief of Police.
- g. If selected as a Homeless Resource Officer, there is authorized pay stipend.
- h. If selected for a specialty position, that requires personnel to be available after hours and weekend coverage, there is authorized on-call pay.

Reporting of Arrests, Convictions, and Court Orders

1002.1 PURPOSE AND SCOPE

The purpose of this policy is to describe the notification requirements and procedures that members must follow when certain arrests, convictions, and court orders restrict their ability to perform the official duties and responsibilities of the South Salt Lake Police Department. This policy will also describe the notification requirements and procedures that certain retired officers must follow when an arrest, conviction, or court order disqualifies them from possessing a firearm.

1002.2 POLICY

The South Salt Lake Police Department requires disclosure of member arrests, convictions, and certain court orders to maintain the high standards, ethics, and integrity in its workforce, and to ensure compatibility with the duties and responsibilities of the [Department/Office].

1002.3 DOMESTIC VIOLENCE CONVICTIONS AND COURT ORDERS

Federal and state law prohibits individuals convicted of certain offenses and individuals subject to certain court orders from lawfully possessing firearms. Such convictions and court orders often involve allegations of the use or attempted use of force, or threatened use of a weapon on any individual in a domestic relationship (e.g., spouse, cohabitant, parent, child) (18 USC § 922; Utah Code 76-11-301 et seq.).

All members and retired officers with identification cards issued by the [Department/Office] are responsible for ensuring that they have not been disqualified from possessing a firearm by any such conviction or court order, and shall promptly report any such conviction or court order to a supervisor, as provided in this policy.

Any person applying for or holding a concealed firearm permit and who is convicted of any offense involving domestic violence may have the permit refused, revoked, or suspended (Utah Code 53-5a-303(2)(a)(vi)).

1002.4 OTHER CRIMINAL CONVICTIONS AND COURT ORDERS

Utah Code 53-6-203 prohibits any person convicted of a felony from being a peace officer in the State of Utah. This prohibition applies regardless of whether the guilt was established by way of a verdict, guilty, or nolo contendere plea.

While legal restrictions may or may not be imposed by statute or by the courts upon conviction of any criminal offense, criminal conduct by members of this [department/office] may be inherently in conflict with law enforcement duties and the public trust, and shall be reported as provided in this policy.

1002.5 REPORTING

All members and all retired officers with identification cards issued by the [Department/Office] shall immediately notify their immediate supervisor (retired officers should immediately notify the Watch

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Reporting of Arrests, Convictions, and Court Orders

Commander or the Chief of Police) in writing of any past or current criminal detention, arrest, charge, or conviction in any state or foreign country, regardless of whether the matter was dropped or rejected, is currently pending or is on appeal, and regardless of the penalty or sentence, if any.

All members and all retired officers with identification cards issued by the [Department/Office] shall immediately notify their supervisors (retired officers should immediately notify the Watch Commander or the Chief of Police) in writing if they become the subject of a domestic violence-related order or any court order that prevents the member or retired officer from possessing a firearm or requires suspension or revocation of applicable POST certification.

Any member whose criminal arrest, conviction, or court order restricts or prohibits that member from fully and properly performing their duties, including carrying a firearm, may be disciplined. This includes but is not limited to being placed on administrative leave, reassignment, and/or termination. Any effort to remove such disqualification or restriction shall remain entirely the responsibility of the member, on their own time and at their own expense.

Any employee failing to provide prompt written notice pursuant to this policy shall be subject to discipline, up to and including termination.

Retired officers may have their identification cards rescinded or modified, as may be appropriate (see the Retiree Concealed Firearms Policy).

Drug- and Alcohol-Free Workplace

1003.1 PURPOSE AND SCOPE

The purpose of this policy is to establish clear and uniform guidelines regarding drugs and alcohol in the workplace.

1003.2 POLICY

It is the policy of this department to provide a drug- and alcohol-free workplace for all members.

1003.3 GENERAL GUIDELINES

Alcohol and drug use in the workplace or on department time can endanger the health and safety of department members and the public.

Members who have consumed an amount of an alcoholic beverage or taken any medication, or combination thereof, that would tend to adversely affect their mental or physical abilities shall not report for duty. Affected members shall notify the Watch Commander or appropriate supervisor as soon as the member is aware that he/she will not be able to report to work. If the member is unable to make the notification, every effort should be made to have a representative contact the supervisor in a timely manner. If the member is adversely affected while on-duty, he/she shall be immediately removed and released from work (see Work Restrictions in this policy).

1003.3.1 USE OF MEDICATIONS

Members should avoid taking any medications that will impair their ability to safely and completely perform their duties. Any member who is medically required or has a need to take any such medication shall report that need to his/her immediate supervisor prior to commencing any on-duty status.

No member shall be permitted to work or drive a vehicle owned or leased by the Department while taking any medication that has the potential to impair his/her abilities, without a written release from his/her physician.

Possession of medical marijuana or being under the influence of marijuana on- or off-duty is prohibited and may lead to disciplinary action.

1003.3.2 MEDICAL CANNABIS

Possession, use, or being under the influence of medical cannabis on-duty is prohibited and may lead to disciplinary action.

1003.4 MEMBER RESPONSIBILITIES

Members shall report for work in an appropriate mental and physical condition. Members are prohibited from purchasing, manufacturing, distributing, dispensing, possessing or using controlled substances or alcohol on department premises or on department time (41 USC § 8103). The lawful possession or use of prescribed medications or over-the-counter remedies is excluded from this prohibition.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Drug- and Alcohol-Free Workplace

Members who are authorized to consume alcohol as part of a special assignment shall not do so to the extent of impairing on-duty performance.

Members shall notify a supervisor immediately if they observe behavior or other evidence that they believe demonstrates that a fellow member poses a risk to the health and safety of the member or others due to drug or alcohol use.

Members are required to notify their immediate supervisors of any criminal drug statute conviction for a violation occurring in the workplace no later than five days after such conviction (41 USC § 8103).

1003.5 EMPLOYEE ASSISTANCE PROGRAM

There may be available a voluntary employee assistance program to assist those who wish to seek help for alcohol and drug problems (41 USC § 8103). Insurance coverage that provides treatment for drug and alcohol abuse also may be available. Employees should contact the Department of Human Resources, their insurance providers or the employee assistance program for additional information. It is the responsibility of each employee to seek assistance before alcohol or drug problems lead to performance problems.

1003.6 WORK RESTRICTIONS

If a member informs a supervisor that he/she has consumed any alcohol, drug or medication that could interfere with a safe and efficient job performance, the member may be required to obtain clearance from his/her physician before continuing to work.

If the supervisor reasonably believes, based on objective facts, that a member is impaired by the consumption of alcohol or other drugs, the supervisor shall prevent the member from continuing work and shall ensure that he/she is safely transported away from the Department.

1003.7 REQUESTING SCREENING TESTS

A supervisor may require an employee to submit to a screening test under any of the following circumstances:

- (a) The supervisor reasonably believes, based upon objective facts, that the employee is under the influence of alcohol or drugs that are impairing his/her ability to perform duties safely and efficiently.
- (b) The employee discharges a firearm, other than by accident, in the performance of his/her duties (excluding training or authorized euthanizing of an animal).
- (c) The employee discharges a firearm issued by the Department while off-duty, resulting in injury, death, or substantial property damage.
- (d) The employee drives a motor vehicle in the performance of his/her duties and becomes involved in an incident that results in bodily injury, death, or substantial damage to property.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Drug- and Alcohol-Free Workplace

1003.7.1 SUPERVISOR RESPONSIBILITY

The supervisor shall prepare a written record documenting the specific facts that led to the decision to require the test, and shall inform the employee in writing of the following:

- (a) The test will be given to detect either alcohol or drugs, or both.
- (b) The result of the test is not admissible in any criminal proceeding against the employee.
- (c) The employee may refuse the test, but refusal may result in dismissal or other disciplinary action.

1003.7.2 DISCIPLINE

An employee may be subject to disciplinary action if he/she:

- (a) Fails or refuses to submit to a screening test.
- (b) After taking a screening test that indicates the presence of a controlled substance, fails to provide proof, within 72 hours after being requested, that he/she took the controlled substance as directed, pursuant to a current and lawful prescription issued in his/her name.

1003.8 COMPLIANCE WITH THE DRUG-FREE WORKPLACE ACT

No later than 30 days following notice of any drug statute conviction for a violation occurring in the workplace involving a member, the Department will take appropriate disciplinary action, up to and including dismissal, and/or requiring the member to satisfactorily participate in a drug abuse assistance or rehabilitation program (41 USC § 8104).

1003.9 CONFIDENTIALITY

The Department recognizes the confidentiality and privacy due to its members. Disclosure of any information relating to substance abuse treatment, except on a need-to-know basis, shall only be with the express written consent of the member involved or pursuant to lawful process.

The written results of any screening tests and all documents generated by the employee assistance program are considered confidential medical records and shall be maintained separately from the employee's other personnel files.

Sick Leave

1004.1 PURPOSE AND SCOPE

This policy provides general guidance regarding the use and processing of sick leave. The accrual and terms of use of sick leave for eligible employees are detailed in the City personnel manual.

This policy is not intended to cover all types of sick or other leaves. For example, employees may be entitled to additional paid or unpaid leave for certain family and medical reasons as provided for in the Family and Medical Leave Act (FMLA) (29 USC § 2601 et seq.).

1004.2 POLICY

It is the policy of the South Salt Lake Police Department to provide eligible employees with a sick leave benefit.

1004.3 USE OF SICK LEAVE

Sick leave is intended to be used for qualified absences. Sick leave is not considered vacation. Abuse of sick leave may result in discipline, denial of sick leave benefits, or both.

Employees on sick leave shall not engage in other employment or self-employment or participate in any sport, hobby, recreational activity or other activity that may impede recovery from the injury or illness (see the Outside Employment Policy).

Qualified appointments should be scheduled during a member's non-working hours when it is reasonable to do so.

1004.3.1 NOTIFICATION

All members should notify the Watch Commander or appropriate supervisor as soon as they are aware that they will not be able to report to work and no less than two hour before the start of their scheduled shifts. If, due to an emergency, a member is unable to contact the supervisor, every effort should be made to have a representative for the member contact the supervisor.

When the necessity to be absent from work is foreseeable, such as planned medical appointments or treatments, the member shall, whenever possible and practicable, provide the Department with no less than 30 days' notice of the impending absence.

Upon return to work, members are responsible for ensuring their time off was appropriately accounted for, and for completing and submitting the required documentation describing the type of time off used and the specific amount of time taken.

Failure to comply with notification requirements, absent extenuating circumstances, may result in the absence being designated as unauthorized and may be subject to administrative review.

1004.4 EXTENDED ABSENCE

Members absent from duty for more than three consecutive days may be required to furnish a statement from a health care provider supporting the need to be absent and/or the ability to return

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Sick Leave

to work. Members on an extended absence shall, if possible, contact their supervisor at specified intervals to provide an update on their absence and expected date of return.

Nothing in this section precludes a supervisor from requiring, with cause, a health care provider's statement for an absence of three or fewer days.

Medical verification requirements shall be applied in a consistent, non-discriminatory manner and may be required when there is a documented pattern of absences, operational necessity or reasonable suspicion of misuse.

All medical documentation shall be handled in accordance with applicable medical privacy laws and maintained separately from personnel files when required.

1004.5 SUPERVISOR RESPONSIBILITIES

The responsibilities of supervisors include, but are not limited to:

- (a) Monitoring and regularly reviewing the attendance of those under their command to ensure that the use of sick leave and absences is consistent with Police Department and City policy.
- (b) Attempting to determine whether an absence of four or more days may qualify as family medical leave and consulting with legal counsel or the Department of Human Resources as appropriate.
- (c) Addressing absences and sick leave use in the member's performance evaluation when excessive or unusual use has:
 - 1. Negatively affected the member's performance or ability to complete assigned duties.
 - 2. Negatively affected department operations.
- (d) When appropriate, counseling members regarding excessive absences and/or inappropriate use of sick leave.
- (e) Referring eligible members to an available employee assistance program when appropriate.
- (f) Supervisors shall ensure that reviews of sick leave usage are based on objective facts, documented patterns and operational impact and shall avoid retaliation or adverse action against members for the lawful and good-faith use of sick leave or protected medical leave.
- (g) Supervisors who become aware of policy violations shall notify up through their chain of command.

Communicable Diseases

1005.1 PURPOSE AND SCOPE

This policy provides general guidelines to assist in minimizing the risk of department members contracting and/or spreading communicable diseases.

1005.1.1 DEFINITIONS

Definitions related to this policy include:

Communicable disease - A human disease caused by microorganisms that are present in and transmissible through human blood, bodily fluid, tissue, or by breathing or coughing. These diseases commonly include, but are not limited to, hepatitis B virus (HBV), HIV and tuberculosis.

Exposure - When an eye, mouth, mucous membrane or non-intact skin comes into contact with blood or other potentially infectious materials, or when these substances are injected or infused under the skin; when an individual is exposed to a person who has a disease that can be passed through the air by talking, sneezing or coughing (e.g., tuberculosis), or the individual is in an area that was occupied by such a person. Exposure only includes those instances that occur due to a member's position at the South Salt Lake Police Department. (See the exposure control plan for further details to assist in identifying whether an exposure has occurred.)

1005.2 POLICY

The South Salt Lake Police Department is committed to providing a safe work environment for its members. Members should be aware that they are ultimately responsible for their own health and safety.

1005.3 EXPOSURE CONTROL OFFICER

The Chief of Police will assign a person as the Exposure Control Officer (ECO). The ECO shall develop an exposure control plan that includes:

- (a) Exposure prevention and decontamination procedures.
- (b) Procedures for when and how to obtain medical attention in the event of an exposure or suspected exposure.
- (c) The provision that [department/office] members will have no-cost access to the appropriate personal protective equipment (PPE) (e.g., gloves, face masks, eye protection, pocket masks) for each member's position and risk of exposure.
- (d) Evaluation of persons in custody for any exposure risk and measures to separate them.
- (e) Compliance with all relevant laws or regulations related to communicable diseases, including:
 - 1. The mandates of the Utah Occupational Safety and Health Act (Utah Code 34A-6-101 et seq.; UAC R614-1-1 et seq.).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Communicable Diseases

2. Reporting known or suspected cases of communicable diseases to the local health department (Utah Code 26B-7-206; UAC R386-702-4).
3. Responding to requests and notifications regarding exposures covered under the Ryan White law (42 USC § 300ff-133; 42 USC § 300ff-136).
4. Exposure control mandates in 29 CFR 1910.1030 (UAC R614-1-4).

The ECO should also act as the liaison with the Utah Occupational Safety and Health Division (UOSH) and may request voluntary compliance inspections. The ECO should annually review and update the exposure control plan and review implementation of the plan.

1005.4 EXPOSURE PREVENTION AND MITIGATION

1005.4.1 GENERAL PRECAUTIONS

All members are expected to use good judgment and follow training and procedures related to mitigating the risks associated with communicable disease. This includes but is not limited to (29 CFR 1910.1030; UAC R614-1-4):

- (a) Stocking disposable gloves, antiseptic hand cleanser, CPR masks, or other specialized equipment in the work area or [department/office] vehicles, as applicable.
- (b) Wearing [department/office]-approved disposable gloves when contact with blood, other potentially infectious materials, mucous membranes, and non-intact skin can be reasonably anticipated.
- (c) Washing hands immediately or as soon as feasible after removal of gloves or other PPE.
- (d) Treating all human blood and bodily fluids/tissue as if it is known to be infectious for a communicable disease.
- (e) Using an appropriate barrier device when providing CPR.
- (f) Using a face mask or shield if it is reasonable to anticipate an exposure to an airborne transmissible disease.
- (g) Decontaminating non-disposable equipment (e.g., flashlight, control devices, clothing, portable radio) as soon as possible if the equipment is a potential source of exposure.
 1. Clothing that has been contaminated by blood or other potentially infectious materials shall be removed immediately or as soon as feasible and stored/decontaminated appropriately.
- (h) Handling all sharps and items that cut or puncture (e.g., needles, broken glass, razors, knives) cautiously and using puncture-resistant containers for their storage and/or transportation.
- (i) Avoiding eating, drinking, smoking, applying cosmetics or lip balm, or handling contact lenses where there is a reasonable likelihood of exposure.
- (j) Disposing of biohazardous waste appropriately or labeling biohazardous material properly when it is stored.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Communicable Diseases

1005.4.2 IMMUNIZATIONS

Members who could be exposed to HBV due to their positions may receive the HBV vaccine and any routine booster at no cost (29 CFR 1910.1030; UAC R614-1-4).

Members shall also be screened for tuberculosis pursuant to the guidelines established by UOSH (UAC R388-804).

1005.5 POST EXPOSURE

1005.5.1 INITIAL POST-EXPOSURE STEPS

Members who experience an exposure or suspected exposure shall (29 CFR 1910.1030; UAC R614-1-4):

- (a) Begin decontamination procedures immediately (e.g., wash hands and any other skin with soap and water, flush mucous membranes with water).
- (b) Obtain medical attention as appropriate.
- (c) Notify a supervisor as soon as practicable.

1005.5.2 REPORTING REQUIREMENTS

The supervisor on-duty shall investigate every exposure or suspected exposure that occurs as soon as possible following the incident. The supervisor shall ensure the following information is documented (29 CFR 1910.1030; UAC R614-1-4):

- (a) Name of the member exposed
- (b) Date and time of the incident
- (c) Location of the incident
- (d) Potentially infectious materials involved and the source of exposure (e.g., identification of the person who may have been the source)
- (e) Work being done during exposure
- (f) How the incident occurred or was caused
- (g) PPE in use at the time of the incident
- (h) Actions taken post-event (e.g., clean-up, notifications)

The supervisor shall advise the member that disclosing the identity and/or infectious status of a source to the public or to anyone who is not involved in the follow-up process is prohibited. The supervisor should complete the incident documentation in conjunction with other reporting requirements that may apply (see the Occupational Disease and Work-Related Injury and Death Reporting Policy).

1005.5.3 MEDICAL CONSULTATION, EVALUATION AND TREATMENT

Department members shall have the opportunity to have a confidential medical evaluation immediately after an exposure and follow-up evaluations as necessary (29 CFR 1910.1030; UAC R614-1-4).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Communicable Diseases

The ECO should request a written opinion/evaluation from the treating medical professional that contains only the following information:

- (a) Whether the member has been informed of the results of the evaluation.
- (b) Whether the member has been notified of any medical conditions resulting from exposure to blood or other potentially infectious materials which require further evaluation or treatment.

No other information should be requested or accepted by the ECO.

1005.5.4 COUNSELING

The [Department/Office] shall provide the member, and the member's family if necessary, the opportunity for counseling and consultation regarding the exposure (29 CFR 1910.1030; UAC R614-1-4).

1005.5.5 SOURCE TESTING

Testing a person for communicable diseases when that person was the source of an exposure should be done when it is desired by the exposed member or when it is otherwise appropriate. Source testing is the responsibility of the ECO. If the ECO is unavailable to seek timely testing of the source, it is the responsibility of the exposed member's supervisor to ensure testing is sought.

Source testing may be achieved by:

- (a) Obtaining consent from the individual.
- (b) Seeking a court order or warrant pursuant to Utah Code 78B-8-402.

Since there is the potential for overlap between the different manners in which source testing may occur, the ECO is responsible for coordinating the testing to prevent unnecessary or duplicate testing.

The ECO should seek the consent of the individual for testing and consult the City Attorney to discuss other options when no statute exists for compelling the source of an exposure to undergo testing if the person refuses.

1005.6 CONFIDENTIALITY OF REPORTS

Medical information shall remain in confidential files and shall not be disclosed to anyone without the member's written consent (except as required by law) (29 CFR 1910.1030; UAC R614-1-4; Utah Code 26B-7-217). Test results from persons who may have been the source of an exposure are to be kept confidential as well.

1005.7 TRAINING

All members shall participate in training regarding communicable diseases commensurate with the requirements of their position. The training (29 CFR 1910.1030; UAC R614-1-4):

- (a) Shall be provided at the time of initial assignment to tasks where an occupational exposure may take place and at least annually after the initial training.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Communicable Diseases

- (b) Shall be provided whenever the member is assigned new tasks or procedures affecting his/her potential exposure to communicable disease.
- (c) Should provide guidance on what constitutes an exposure, what steps can be taken to avoid an exposure and what steps should be taken if a suspected exposure occurs.

Smoking and Tobacco Use

1006.1 PURPOSE AND SCOPE

This policy establishes limitations on smoking and the use of tobacco products by members and others while on-duty or while in South Salt Lake Police Department facilities or vehicles.

For the purposes of this policy, smoking and tobacco use includes, but is not limited to, any tobacco product, such as cigarettes, cigars, pipe tobacco, snuff, tobacco pouches and chewing tobacco, as well as any device intended to simulate smoking, such as an electronic cigarette or personal vaporizer.

1006.2 POLICY

The South Salt Lake Police Department recognizes that tobacco use is a health risk and can be offensive to others. Smoking and tobacco use also presents an unprofessional image for the [Department/Office] and its members. Therefore smoking and tobacco use is prohibited by members and visitors in all [department/office] facilities, buildings, and vehicles, and as is further outlined in this policy (Utah Code 26B-7-503).

Personnel Complaints

1007.1 PURPOSE AND SCOPE

This policy provides guidelines for the reporting, investigation and disposition of complaints regarding the conduct of members of the South Salt Lake Police Department. This policy shall not apply to any questioning, counseling, instruction, informal verbal admonishment or other routine or unplanned contact of a member in the normal course of duty, by a supervisor or any other member, nor shall this policy apply to a criminal investigation.

1007.1.1 CATEGORIES OF COMPLAINTS AND INVESTIGATIONS

- (a) Complaints and/or investigations shall be classified as one of three (3) categories:
 - 1. Category I - Complaints/investigations handled by the Professional Standards Unit may include, but are not limited to:
 - (a) Situations in which an employee has been killed or injured by the willful or deliberate act of another person.
 - (b) Situations in which a citizen has been injured or killed by an employee, whether on- or off-duty if under color of police authority, or if there is suspicion of criminal intent, or violation of statute by the employee.
 - (c) Situations on- or off-duty involving the discharge of a firearm by an employee in other than lawful sport activity or at an approved firing range, when personal injury or property damage has occurred.
 - (d) Allegations of false arrest or excessive force which may result in civil litigation against the employee or the police department.
 - (e) Alleged or suspected breach of integrity or moral misconduct that affects the department.
 - (f) Complaints alleging criminal conduct by a police department employee.
 - (g) Allegations regarding the use of racial slurs by a police department employee.
 - (h) Allegations of civil rights violations committed by a police department employee.
 - (i) Allegation of or incidents involving a violation of department or city policy, as directed by the Chief of Police or his/her designee.
 - 2. Category II - Complaints/investigations of a minor or informal nature may be handled by handled by a supervisor and include, but are not limited to:
 - (a) A complaint regarding organizational procedures.
 - (b) Legal issues.
 - (c) Policy interpretations.
 - (d) Allegations of rudeness or discourtesy by a police department employee.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personnel Complaints

- (e) Traffic violations by a police department employee.
 - (f) Violations of department or city policy that do not include a use of deadly force.
 - (g) Allegations of errors or inaccuracies in a written report or traffic citation.
 - (h) If a supervisor determines that the complaint is based on a lack of information or understanding on the part of the complainant, the complaint may be resolved without a formal investigation.
 - 3. Category III - Background investigations for potential police department employees.
- (b) If an officer or employee is alleged to be involved in a Category I complaint, timely notification to the Deputy Chief and Chief is required.

1007.2 POLICY

The South Salt Lake Police Department takes seriously all complaints regarding the service provided by the [Department/Office] and the conduct of its members.

The [Department/Office] will accept and address all complaints of misconduct in accordance with this policy and applicable federal, state, and local law, municipal and county rules, and the requirements of any memorandum of understanding or collective bargaining agreement.

It is also the policy of this [department/office] to ensure that the community can report misconduct without concern for reprisal or retaliation.

1007.3 PERSONNEL COMPLAINTS

Personnel complaints include any allegation of misconduct or improper job performance that, if true, would constitute a violation of [department/office] policy or of federal, state, or local law, policy, or rule. Personnel complaints may be generated internally or by the public.

Inquiries about conduct or performance that, if true, would not violate [department/office] policy or federal, state, or local law, policy, or rule may be handled informally by a supervisor and shall not be considered a personnel complaint. Such inquiries generally include clarification regarding policy, procedures, or the response to specific incidents by the [Department/Office].

1007.3.1 COMPLAINT CLASSIFICATIONS

Personnel complaints shall be classified in one of the following categories:

Informal - A matter in which the Watch Commander is satisfied that appropriate action has been taken by a supervisor of rank greater than the accused member.

Formal - A matter in which a supervisor determines that further action is warranted. Such complaints may be investigated by a supervisor of rank greater than the accused member or referred to the Professional Standards Unit, depending on the seriousness and complexity of the investigation.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personnel Complaints

Incomplete - A matter in which the complaining party either refuses to cooperate or becomes unavailable after diligent follow-up investigation. At the discretion of the assigned supervisor or the Professional Standards Unit, such matters may be further investigated depending on the seriousness of the complaint and the availability of sufficient information.

1007.3.2 SOURCES OF COMPLAINTS

The following applies to the source of complaints:

- (a) Individuals from the public may make complaints in any form, including in writing, by email, in person, or by telephone.
- (b) Any [department/office] member becoming aware of alleged misconduct shall immediately notify a supervisor.
- (c) Supervisors shall initiate a complaint based upon observed misconduct or receipt from any source alleging misconduct that, if true, could result in disciplinary action.
- (d) Anonymous and third-party complaints should be accepted and investigated to the extent that sufficient information is provided.
- (e) Tort claims and lawsuits may generate a personnel complaint.

1007.4 AVAILABILITY AND ACCEPTANCE OF COMPLAINTS

1007.4.1 COMPLAINT FORMS

Personnel complaint forms will be maintained in a clearly visible location in the public area of the police facility and be accessible through the [department/office] website. Forms may also be available at other City facilities.

Personnel complaint forms in languages other than English may also be provided, as determined necessary or practicable.

1007.4.2 ACCEPTANCE

All complaints will be courteously accepted by any [department/office] member and promptly given to the appropriate supervisor. Although written complaints are preferred, a complaint may also be filed orally, either in person or by telephone. Such complaints will be directed to a supervisor. If a supervisor is not immediately available to take an oral complaint, the receiving member shall obtain contact information sufficient for the supervisor to contact the complainant. The supervisor, upon contact with the complainant, shall complete and submit a complaint form as appropriate.

Although not required, complainants should be encouraged to file complaints in person so that proper identification, signatures, photographs, or physical evidence may be obtained as necessary.

1007.5 DOCUMENTATION

Supervisors shall ensure that all formal and informal complaints are documented on a complaint form. The supervisor shall ensure that the nature of the complaint is defined as clearly as possible.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personnel Complaints

All complaints and inquiries should also be documented in a log that records and tracks complaints. The log shall include the nature of the complaint and the actions taken to address the complaint. On an annual basis, the [Department/Office] should audit the log and send an audit report to the Chief of Police or the authorized designee.

1007.6 ADMINISTRATIVE INVESTIGATIONS

Allegations of misconduct will be administratively investigated as follows.

1007.6.1 SUPERVISOR RESPONSIBILITIES

In general, the primary responsibility for the investigation of a personnel complaint shall rest with the member's immediate supervisor, unless the supervisor is the complainant, or the supervisor is the ultimate decision-maker regarding disciplinary action or has any personal involvement regarding the alleged misconduct. The Chief of Police or the authorized designee may direct that another supervisor investigate any complaint.

A supervisor who becomes aware of alleged misconduct shall take reasonable steps to prevent aggravation of the situation.

The Chief of Police or any other supervisor who is made aware of an allegation against a certified peace officer or dispatcher employed by the South Salt Lake Police Department shall conduct an administrative or internal investigation and report substantiated allegations to the Division of Peace Officer Standards and Training (POST) within 30 days (Utah Code 53-6-211; Utah Code 53-6-309; UAC R728-409-18).

If an officer or dispatcher who is the subject of the investigation resigns, retires, or otherwise separates from the agency before the conclusion of the investigation, the Chief of Police shall report the allegations and any investigation results to POST (Utah Code 53-6-211; Utah Code 53-6-309; UAC R728-409-18).

The Chief of Police shall notify POST within 30 days after the officer's termination date if the date occurs during an open internal investigation for an alleged violation of Utah Code 53-6-211(1) (Utah Code 53-6-209).

If the South Salt Lake Police Department receives credible allegations and opens an internal investigation within two years after the day of an officer's termination date, the Chief of Police shall provide notice 30 days after the day of opening the investigation and an estimated date of completion to POST. If the allegations involve violations of Utah Code 53-6-211(1), whether or not they result in an internal investigation, the Chief of Police shall notify POST (Utah Code 53-6-209).

The responsibilities of supervisors include but are not limited to:

- (a) Ensuring that upon receiving or initiating any formal complaint, a complaint form is completed.
 1. The original complaint form will be directed to the Watch Commander of the accused member, via the chain of command, who will take appropriate action and/or determine who will have responsibility for the investigation.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personnel Complaints

2. In circumstances where the integrity of the investigation could be jeopardized by reducing the complaint to writing or where the confidentiality of a complainant is at issue, a supervisor shall orally report the matter to the member's Division Commander or the Chief of Police, who will initiate appropriate action.
- (b) Responding to all complainants in a courteous and professional manner.
- (c) Resolving those personnel complaints that can be resolved immediately.
 1. Follow-up contact with the complainant should be made within 24 hours of the [Department/Office] receiving the complaint.
 2. If the matter is resolved and no further action is required, the supervisor will note the resolution on a complaint form and forward the form to the Watch Commander.
- (d) Ensuring that upon receipt of a complaint involving allegations of a potentially serious nature, the Watch Commander and Chief of Police are notified via the chain of command as soon as practicable.
- (e) Promptly contacting the Department of Human Resources and the Watch Commander for direction regarding the supervisor's role in addressing a complaint that relates to sexual, racial, ethnic, or other forms of prohibited harassment or discrimination.
- (f) Forwarding unresolved personnel complaints to the Watch Commander, who will determine whether to contact the complainant or assign the complaint for investigation.
- (g) Informing the complainant of the investigator's name and the complaint number within three days after assignment.
- (h) Investigating a complaint as follows:
 1. Making reasonable efforts to obtain names, addresses, and telephone numbers of witnesses.
 2. When appropriate, ensuring immediate medical attention is provided and photographs of alleged injuries and accessible uninjured areas are taken.
- (i) Ensuring that the procedural rights of the accused member are followed.
- (j) Ensuring interviews of the complainant are generally conducted during reasonable hours.

1007.6.2 ADMINISTRATIVE INVESTIGATION PROCEDURES

Whether conducted by a supervisor or a member of the Professional Standards Unit, the following applies to employees:

- (a) Interviews of an accused employee shall be conducted during reasonable hours and preferably when the employee is on-duty. If the employee is off-duty, he/she shall be compensated.
- (b) Unless waived by the employee, interviews of an accused employee shall be at the South Salt Lake Police Department or other reasonable and appropriate place.
- (c) No more than two interviewers should ask questions of an accused employee.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personnel Complaints

- (d) Prior to any interview, an employee should be informed of the nature of the investigation.
- (e) All interviews should be for a reasonable period and the employee's personal needs should be accommodated.
- (f) No employee should be subjected to offensive or threatening language, nor shall any promises, rewards or other inducements be used to obtain answers.
- (g) Any employee refusing to answer questions directly related to the investigation may be ordered to answer questions administratively and may be subject to discipline for failing to do so.
 - 1. An employee should be given an order to answer questions in an administrative investigation that might incriminate the member in a criminal matter only after the employee has been given a *Garrity* advisement and after the investigator has consulted with the prosecuting agency. Administrative investigators should consider the impact that compelling a statement from the employee may have on any related criminal investigation and should take reasonable steps to avoid creating any foreseeable conflicts between the two related investigations. This may include conferring with the person in charge of the criminal investigation (e.g., discussion of processes, timing, implications).
 - 2. No information or evidence administratively coerced from an employee may be provided to anyone involved in conducting the criminal investigation or to any prosecutor.
- (h) The interviewer should record all interviews of employees and witnesses. The employee may also record the interview. If the employee has been previously interviewed, a copy of that recorded interview shall be provided to the employee prior to any subsequent interview.
- (i) All employees subjected to interviews that could result in discipline have the right to have an uninvolved representative present during the interview. However, in order to maintain the integrity of each individual's statement, involved employees shall not consult or meet with a representative or attorney collectively or in groups prior to being interviewed.
- (j) All employees shall provide complete and truthful responses to questions posed during interviews.
- (k) No employee may be compelled to submit to a polygraph examination, nor shall any refusal to submit to such examination be mentioned in any investigation.

1007.6.3 ADMINISTRATIVE INVESTIGATION FORMAT

Formal investigations of personnel complaints shall be thorough, complete and essentially follow this format:

Introduction - Include the identity of the members, the identity of the assigned investigators, the initial date and source of the complaint.

Synopsis - Provide a brief summary of the facts giving rise to the investigation.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personnel Complaints

Summary - List the allegations separately, including applicable policy sections, with a brief summary of the evidence relevant to each allegation. A separate recommended finding should be provided for each allegation.

Evidence - Each allegation should be set forth with the details of the evidence applicable to each allegation provided, including comprehensive summaries of member and witness statements. Other evidence related to each allegation should also be detailed in this section.

Conclusion - A recommendation regarding further action or disposition should be provided.

Exhibits - A separate list of exhibits (e.g., recordings, photos, documents) should be attached to the report.

1007.6.4 DISPOSITIONS

Each personnel complaint shall be classified with one of the following dispositions:

Unfounded - When the investigation discloses that the alleged acts did not occur or did not involve [department/office] members. Complaints that are determined to be frivolous will fall within the classification of unfounded.

Exonerated - When the investigation discloses that the alleged act occurred but that the act was justified, lawful and/or proper.

Not sustained - When the investigation discloses that there is insufficient evidence to sustain the complaint or fully exonerate the member.

Sustained - When the investigation discloses sufficient evidence to establish that the act occurred and that it constituted misconduct.

If an investigation discloses misconduct or improper job performance that was not alleged in the original complaint, the investigator shall take appropriate action with regard to any additional allegations.

1007.6.5 COMPLETION OF INVESTIGATIONS

Every investigator or supervisor assigned to investigate a personnel complaint or other alleged misconduct shall proceed with due diligence in an effort to complete the investigation within one year from the date of discovery by an individual authorized to initiate an investigation.

1007.6.6 NOTICE TO COMPLAINANT OF INVESTIGATION STATUS

The member conducting the investigation should provide the complainant with periodic updates on the status of the investigation, as appropriate.

1007.7 ADMINISTRATIVE SEARCHES

Assigned lockers, storage spaces and other areas, including desks, offices and vehicles, may be searched as part of an administrative investigation upon a reasonable suspicion of misconduct.

Such areas may also be searched any time by a supervisor for non-investigative purposes, such as obtaining a needed report, radio or other document or equipment.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personnel Complaints

1007.8 ADMINISTRATIVE LEAVE

When a complaint of misconduct is of a serious nature, or when circumstances indicate that allowing the accused to continue to work would adversely affect the mission of the [Department/Office], the Chief of Police or the authorized designee may temporarily assign an accused employee to administrative leave. Any employee placed on administrative leave:

- (a) May be required to relinquish any [department/office] badge, identification, assigned weapons, and any other [department/office] equipment.
- (b) Shall be required to continue to comply with all policies and lawful orders of a supervisor.
- (c) May be temporarily reassigned to a different shift, generally a normal business-hours shift, during the investigation. The employee may be required to remain available for contact at all times during such shift, and will report as ordered.

1007.9 CRIMINAL INVESTIGATION

Where a member is accused of potential criminal conduct, a separate supervisor or investigator shall be assigned to investigate the criminal allegations apart from any administrative investigation. Any separate administrative investigation may parallel a criminal investigation.

The Chief of Police shall be notified as soon as practicable when a member is accused of criminal conduct. The Chief of Police may request a criminal investigation by an outside law enforcement agency.

A member accused of criminal conduct shall be provided with all rights afforded to a civilian. The member should not be administratively ordered to provide any information in the criminal investigation.

The South Salt Lake Police Department may release information concerning the arrest or detention of any member, including an officer, that has not led to a conviction. No disciplinary action should be taken until an independent administrative investigation is conducted.

1007.10 POST-ADMINISTRATIVE INVESTIGATION PROCEDURES

Upon completion of a formal investigation, an investigation report should be forwarded to the Chief of Police through the chain of command. Each level of command should review the report and include their comments in writing before forwarding the report. The Chief of Police may accept or modify any classification or recommendation for disciplinary action.

1007.10.1 DIVISION COMMANDER RESPONSIBILITIES

Upon receipt of any completed personnel investigation, the Division Commander of the involved member shall review the entire investigative file, the member's personnel file and any other relevant materials.

The Division Commander may make recommendations regarding the disposition of any allegations and the amount of discipline, if any, to be imposed.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personnel Complaints

Prior to forwarding recommendations to the Chief of Police, the Division Commander may return the entire investigation to the assigned investigator or supervisor for further investigation or action.

When forwarding any written recommendation to the Chief of Police, the Division Commander shall include all relevant materials supporting the recommendation. Actual copies of a member's existing personnel file need not be provided and may be incorporated by reference.

1007.10.2 CHIEF OF POLICE RESPONSIBILITIES

Upon receipt of any written recommendation for disciplinary action, the Chief of Police shall review the recommendation and all accompanying materials. The Chief of Police may modify any recommendation and/or may return the file to the Division Commander for further investigation or action.

Once the Chief of Police is satisfied that no further investigation or action is required by staff, the Chief of Police shall determine the amount of discipline, if any that should be imposed. In the event disciplinary action is proposed, the Chief of Police shall provide the member with a written notice and the following:

- (a) Access to all of the materials considered by the Chief of Police, except materials protected by attorney client privilege, in recommending the proposed discipline.
- (b) An opportunity to respond in writing to the Chief of Police within 10 days of receiving the notice.
 1. Upon a showing of good cause by the member, the Chief of Police may grant a reasonable extension of time for the member to respond.

Once the member has completed his/her response or if the member has elected to waive any such response, the Chief of Police shall consider all information received in regard to the recommended discipline. The Chief of Police shall render a timely written decision to the member and specify the grounds and reasons for discipline and the effective date of the discipline. Once the Chief of Police has issued a written decision, the discipline shall become effective.

1007.10.3 NOTICE OF FINAL DISPOSITION TO THE COMPLAINANT

The Chief of Police or the authorized designee should ensure that the complainant is notified of the disposition (i.e., sustained, not sustained, exonerated, unfounded) of the complaint.

1007.10.4 DISCIPLINE

Disciplinary actions should be administered progressively and according to the seriousness of the violation. Disciplinary action may include the following:

- Counseling
- Oral reprimand
- Letter of reprimand
- Loss of leave
- Suspension

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personnel Complaints

- Demotion
- Termination of employment

1007.11 PRE-DISCIPLINE EMPLOYEE RESPONSE

The pre-discipline process is intended to provide the accused employee with an opportunity to present a written or oral response to the Chief of Police after having had an opportunity to review the supporting materials and prior to imposition of any recommended discipline. The employee shall consider the following:

- (a) The response is not intended to be an adversarial or formal hearing.
- (b) Although the employee may be represented by an uninvolved representative or legal counsel, the response is not designed to accommodate the presentation of testimony or witnesses.
- (c) The employee may suggest that further investigation could be conducted or the employee may offer any additional information or mitigating factors for the Chief of Police to consider.
- (d) In the event that the Chief of Police elects to conduct further investigation, the employee shall be provided with the results prior to the imposition of any discipline.
- (e) The employee may thereafter have the opportunity to further respond orally or in writing to the Chief of Police on the limited issues of information raised in any subsequent materials.

1007.12 RESIGNATIONS/RETIREMENTS PRIOR TO DISCIPLINE

In the event that a member tenders a written resignation or notice of retirement prior to the imposition of discipline, it shall be noted in the file. The tender of a resignation or retirement by itself shall not serve as grounds for the termination of any pending investigation or discipline.

1007.13 POST-DISCIPLINE APPEAL RIGHTS

An employee discharged, transferred to another position with less pay, or suspended without pay for more than two days may, within 10 days from the issuance by the Chief of Police of the order of discharge, transfer, or suspension, appeal to an appeal board or a hearing officer if one has been established. However, if the [Department/Office] has established an internal grievance procedure, the employee must exhaust all available grievance remedies before making such an appeal (Utah Code 10-3-1106).

The employee may appear in person and may have counsel and a public hearing. The findings and decision of the appeal board or hearing officer shall be final.

Any final action or order of the appeal board or hearing officer may be appealed to the Court of Appeals within 30 days of the issuance of the final action or order of the appeal board or hearing officer.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personnel Complaints

1007.14 PROBATIONARY EMPLOYEES AND OTHER MEMBERS

At-will and probationary employees and members other than non-probationary employees may be disciplined and/or released from employment without adherence to any of the procedures set out in this policy, and without notice or cause at any time. These individuals are not entitled to any rights under this policy. However, any of these individuals released for misconduct should be afforded an opportunity solely to clear their names through a liberty interest hearing, which shall be limited to a single appearance before the Chief of Police or the authorized designee.

In cases where the individual has been absent for more than a week or when additional time to review the individual is considered to be appropriate, the probationary period may be extended at the discretion of the Chief of Police.

1007.15 RETENTION OF PERSONNEL INVESTIGATION FILES

All personnel complaints shall be maintained in accordance with the established records retention schedule and as described in the Personnel Records Policy.

1007.16 NOTICE OF SUSTAINED MISCONDUCT INVOLVING BRADY MATERIAL

If an allegation of misconduct involving *Brady* material is sustained, the Chief of Police or the authorized designee shall report the findings of the investigation to the county attorney or Utah Attorney General as applicable (Utah Code 53-25-1003).

Seat Belts

1008.1 PURPOSE AND SCOPE

This policy establishes guidelines for the use of seat belts and child restraints. This policy will apply to all members operating or riding in department vehicles.

Guidance for transporting persons in custody may be found in the Transporting Persons in Custody and Handcuffing and Restraints policies.

1008.1.1 DEFINITIONS

Definitions related to this policy include:

Child restraint system - An infant or child passenger restraint system that meets Federal Motor Vehicle Safety Standards (FMVSS) and Regulations set forth in 49 CFR 571.213 (Utah Code 41-6a-1601).

1008.2 POLICY

It is the policy of the South Salt Lake Police Department that members use safety and child restraint systems to reduce the possibility of death or injury in a motor vehicle collision.

1008.3 WEARING OF SAFETY RESTRAINTS

All members shall wear properly adjusted safety restraints when operating or riding in a seat equipped with restraints, in any vehicle owned, leased or rented by this department, while on- or off-duty, or in any privately owned vehicle while on-duty. The member driving such a vehicle shall ensure that all other occupants, including non-members of the Department, are properly restrained (Utah Code 41-6a-1803).

Exceptions to the requirement to wear safety restraints may be made only in exceptional situations where, due to unusual circumstances, wearing a seat belt would endanger the department member or the public. Members must be prepared to justify any deviation from this requirement.

1008.4 TRANSPORTING CHILDREN

A child younger than 8 years of age shall be secured using a child restraint system in the manner prescribed by the manufacturer of the system unless an exemption exists due to the child's height (Utah Code 41-6a-1803).

Rear seat passengers in a cage-equipped vehicle may have reduced clearance, which requires careful seating and positioning of seat belts. Due to this reduced clearance, and if permitted by law, children and any child restraint system may be secured in the front seat of such vehicles provided this positioning meets federal safety standards and the vehicle and child restraint system manufacturer's design and use recommendations. In the event that a child is transported in the front seat of a vehicle, the seat should be pushed back as far as possible and the passenger-side airbag should be deactivated. If this is not possible, members should arrange alternate transportation when feasible.

There are several child car seats at the public safety building for transportation use.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Seat Belts

1008.5 INOPERABLE SEAT BELTS

Department vehicles shall not be operated when the seat belt in the driver's position is inoperable. Persons shall not be transported in a seat in which the seat belt is inoperable.

Department vehicle seat belts shall not be modified, removed, deactivated or altered in any way, except by the vehicle maintenance and repair staff, who shall do so only with the express authorization of the Chief of Police.

Members who discover an inoperable restraint system shall report the defect to the appropriate supervisor. Prompt action will be taken to replace or repair the system.

1008.6 VEHICLES MANUFACTURED WITHOUT SEAT BELTS

Vehicles manufactured and certified for use without seat belts or other restraint systems are subject to the manufacturer's operator requirements for safe use.

1008.7 VEHICLE AIRBAGS

In all vehicles equipped with airbag restraint systems, the system will not be tampered with or deactivated, except when transporting children as written elsewhere in this policy. All equipment installed in vehicles equipped with airbags will be installed as per the vehicle manufacturer specifications to avoid the danger of interfering with the effective deployment of the airbag device.

1008.8 UTAH STATE LAW 41-6A-1803 EFFECTIVE 5/1/2024

[See attachment: Utah 41-6a-1803 effective May 2024.pdf](#)

Body Armor

1009.1 PURPOSE AND SCOPE

The purpose of this policy is to provide law enforcement officers with guidelines for the proper use of body armor.

1009.2 POLICY

It is the policy of the South Salt Lake Police Department to maximize officer safety through the use of body armor in combination with prescribed safety procedures. While body armor provides a significant level of protection, it is not a substitute for the observance of officer safety procedures.

1009.3 ISSUANCE OF BODY ARMOR

The Administration supervisor shall ensure that body armor is issued to all officers when the officer begins service at the South Salt Lake Police Department and that, when issued, the body armor meets or exceeds the standards of the National Institute of Justice.

The Administration supervisor shall establish a body armor replacement schedule and ensure that replacement body armor is issued pursuant to the schedule or whenever the body armor becomes worn or damaged to the point that its effectiveness or functionality has been compromised.

1009.3.1 USE OF SOFT BODY ARMOR

Generally, the use of body armor is required in accordance with manufacturer guidelines and subject to the following:

- (a) Officers shall only wear agency-approved body armor.
- (b) Officers shall wear body armor anytime they are in a situation where they could reasonably be expected to take enforcement action.
- (c) Officers may be excused from wearing body armor when they are functioning primarily in an administrative or support capacity and could not reasonably be expected to take enforcement action.
- (d) Body armor shall be worn when an officer is working in uniform or taking part in [department/office] range training.
- (e) An officer may be excused from wearing body armor when they are involved in undercover or plainclothes work that their supervisor determines could be compromised by wearing body armor, or when a supervisor determines that other circumstances make it inappropriate to mandate wearing body armor.

1009.3.2 INSPECTIONS OF BODY ARMOR

Supervisors should ensure that body armor is worn and maintained in accordance with this policy through routine observation and periodic documented inspections. Annual inspections of body armor should be conducted by an authorized designee for fit, cleanliness and signs of damage, abuse and wear.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Body Armor

1009.3.3 CARE AND MAINTENANCE OF SOFT BODY ARMOR

Soft body armor should never be stored for any period of time in an area where environmental conditions (e.g., temperature, light, humidity) are not reasonably controlled (e.g., normal ambient room temperature/humidity conditions), such as in automobiles or automobile trunks.

Soft body armor should be cared for and cleaned pursuant to the manufacturer's care instructions provided with the soft body armor. The instructions can be found on labels located on the external surface of each ballistic panel. The carrier should also have a label that contains care instructions. Failure to follow these instructions may damage the ballistic performance capabilities of the armor. If care instructions for the soft body armor cannot be located, contact the manufacturer to request care instructions.

Soft body armor should not be exposed to any cleaning agents or methods not specifically recommended by the manufacturer, as noted on the armor panel label.

1009.4 FIREARMS SUPERVISOR RESPONSIBILITIES

The Firearms Supervisor should:

- (a) Monitor technological advances in the body armor industry for any appropriate changes to Department approved body armor.
- (b) Assess weapons and ammunition currently in use and the suitability of approved body armor to protect against those threats.
- (c) Provide training that educates officers about the safety benefits of wearing body armor.

Personnel Records

1010.1 PURPOSE AND SCOPE

This policy governs maintenance and access to personnel records. Personnel records include any file maintained under an individual member's name.

1010.2 DEPARTMENT FILE

The department file shall be maintained as a record of a person's employment/appointment with this department. The department file should contain, at a minimum:

- (a) Personal data, including photographs, marital status, names of family members, educational and employment history or similar information. A photograph of the member should be permanently retained.
- (b) Election of employee benefits.
- (c) Personnel action reports reflecting assignments, promotions and other changes in employment/appointment status. These should be permanently retained.
- (d) Original performance evaluations. These should be permanently maintained.
- (e) Discipline records, including copies of sustained personnel complaints.
- (f) Adverse comments such as supervisor notes or memos may be retained in the department file after the member has had the opportunity to read and initial the comment.
 - 1. Once a member has had an opportunity to read and initial any adverse comment, the member shall be given the opportunity to respond in writing to the adverse comment.
 - 2. Any member response shall be attached to and retained with the original adverse comment.
 - 3. If a member refuses to initial or sign an adverse comment, at least one supervisor should note the date and time of such refusal on the original comment. Such a refusal, however, shall not be deemed insubordination, nor shall it prohibit the entry of the adverse comment into the member's file.
- (g) Commendations and awards.
- (h) Any other information, the disclosure of which would constitute an unwarranted invasion of personal privacy.

1010.3 DIVISION FILE

Division files may be separately maintained internally by a member's supervisor for the purpose of completing timely performance evaluations. The Division file may contain supervisor comments, notes, notices to correct and other materials that are intended to serve as a foundation for the completion of timely performance evaluations.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personnel Records

1010.4 TRAINING FILE

An individual training file shall be maintained by the Training Coordinator for each member. Training files will contain records of all training; original or photocopies of available certificates, transcripts, diplomas and other documentation; and education and firearms qualifications. Training records may also be created and stored remotely, either manually or automatically (e.g., Daily Training Bulletin (DTB) records).

- (a) The involved member is responsible for providing the Training Coordinator or immediate supervisor with evidence of completed training/education in a timely manner.
- (b) The Training Coordinator or supervisor shall ensure that copies of such training records are placed in the member's training file.

1010.5 MEMBER ACCESS TO HIS/HER OWN PERSONNEL RECORDS

Any member may request access to his/her own personnel records during the normal business hours of those responsible for maintaining such files. Any member seeking the removal of any item from his/her personnel records shall file a written request to the Chief of Police through the chain of command. The Department shall remove any such item if appropriate, or within 30 days provide the member with a written explanation of why the contested item will not be removed. If the contested item is not removed from the file, the member's request and the written response from the Department shall be retained with the contested item in the member's corresponding personnel record.

Members may be restricted from accessing files containing any of the following information:

- (a) An ongoing internal affairs investigation to the extent that it could jeopardize or compromise the investigation pending final disposition or notice to the member of the intent to discipline.
- (b) Confidential portions of internal affairs files that have not been sustained against the member.
- (c) Criminal investigations involving the member.
- (d) Letters of reference concerning employment/appointment, licensing or issuance of permits regarding the member.
- (e) Any portion of a test document, except the cumulative total test score for either a section of the test document or for the entire test document.
- (f) Materials used by the Department for staff management planning, including judgments or recommendations concerning future salary increases and other wage treatments, management bonus plans, promotions and job assignments or other comments or ratings used for department planning purposes.
- (g) Information of a personal nature about a person other than the member if disclosure of the information would constitute a clearly unwarranted invasion of the other person's privacy.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personnel Records

- (h) Records relevant to any other pending claim between the Department and the member that may be discovered in a judicial proceeding.

1010.6 RETENTION AND PURGING

Unless provided otherwise in this policy, personnel records shall be maintained in accordance with the established records retention schedule.

- (a) During the preparation of each member's performance evaluation, all personnel complaints and disciplinary actions should be reviewed to determine the relevancy, if any, to progressive discipline, training and career development. Each supervisor responsible for completing the member's performance evaluation should determine whether any prior sustained disciplinary file should be retained beyond the required period for reasons other than pending litigation or other ongoing legal proceedings.
- (b) If a supervisor determines that records of prior discipline should be retained beyond the required period, approval for such retention should be obtained through the chain of command from the Chief of Police.
- (c) If, in the opinion of the Chief of Police, a personnel complaint or disciplinary action maintained beyond the required retention period is no longer relevant, all records of such matter may be destroyed in accordance with the established records retention schedule.

1010.7 POLICY

It is the policy of this department to maintain personnel records and preserve the confidentiality of personnel records pursuant to the Constitution and the laws of Utah (Utah Code 63G-2-302 et seq.).

1010.8 INTERNAL AFFAIRS FILE

Internal affairs files shall be maintained under the exclusive control of the Professional Standards Unit in conjunction with the office of the Chief of Police. Access to these files may only be approved by the Chief of Police or the Professional Standards Unit supervisor.

These files shall contain the complete investigation of all formal complaints of member misconduct, regardless of disposition. Investigations of complaints that result in the following findings shall not be placed in the member's department file but will be maintained in the internal affairs file:

- (a) Not sustained
- (b) Unfounded
- (c) Exonerated

1010.9 MEDICAL FILE

A medical file shall be maintained separately from all other personnel records and shall contain all documents relating to the member's medical condition and history, including but not limited to:

- (a) Materials relating to a medical leave of absence, including leave under the Family and Medical Leave Act (FMLA).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personnel Records

- (b) Documents relating to workers' compensation claims or the receipt of short- or long-term disability benefits.
- (c) Fitness-for-duty examinations, psychological and physical examinations, follow-up inquiries and related documents.
- (d) Medical release forms, doctor's slips and attendance records that reveal a member's medical condition.
- (e) Any other documents or materials that reveal the member's medical history or medical condition, including past, present or future anticipated mental, psychological or physical limitations.

1010.10 SECURITY

Personnel records should be maintained in a secured location and locked either in a cabinet or access-controlled room. Personnel records maintained in an electronic format should have adequate password protection.

Personnel records are subject to disclosure only as provided in this policy, the Records Maintenance and Release Policy or according to applicable discovery procedures.

Nothing in this policy is intended to preclude review of personnel records by the Mayor, City Attorney or other attorneys or representatives of the City in connection with official business.

1010.10.1 REQUESTS FOR DISCLOSURE

Any member receiving a request for a personnel record shall promptly notify the Records Officer or other person charged with the maintenance of such records.

Upon receipt of any such request, the responsible person shall notify the affected member as soon as practicable that such a request has been made.

The responsible person shall further ensure that an appropriate response to the request is made in a timely manner, consistent with applicable law. In many cases, this may require assistance of available legal counsel.

All requests for disclosure that result in access to a member's personnel records shall be logged in the corresponding file.

1010.10.2 RELEASE OF PERSONNEL INFORMATION

Information such as the member's medical information, or the home address, telephone number and Social Security number of the member or of the member's family, that is contained in a personnel record is confidential and may not be released (Utah Code 63G-2-302; Utah Code 63G-2-303; Utah Code 63G-2-304).

The Department may release any factual information concerning a disciplinary investigation if the member who is the subject of the investigation (or the member's representative) publicly makes a statement that is published in the media and that the member (or representative) knows to be false. The disclosure of such information, if any, shall be limited to facts that refute any such false statement.

Employee/Supervisor Specialty Assignments and Rotations

1011.1 PURPOSE AND SCOPE

The South Salt Lake Police Department allows its sworn personnel to be assigned to specialized assignments to provide opportunities for personal growth, improved job satisfaction, and increased performance effectiveness. As employees acquire additional skills, knowledge and abilities, the department benefits from an expanded pool of employees who are prepared to assume a variety of duties and responsibilities.

1011.2 POLICY

- (a) The South Salt Lake City Police Department believes in career development for employees.
 - 1. To support this belief, there is a three (3) year minimum commitment and a five (5) year recommended rotation policy to guide movement within different units and specialties.
 - 2. Once an employee/supervisor reaches a recommended rotation, and the transfer of the employee has been approved, the employee's supervisor, the employee, and the affected division commander, will work out a reasonable transfer process.
 - 3. A transitional training period should be conducted for the employee selected to fill the assignment, with the employee leaving the assignment, prior to the scheduled rotation date.
 - 4. Any employee/supervisor who is selected for a specialty unit will not be eligible for selection to another unit or specialty until the three (3) year minimum commitment from the date of placement period has passed.
 - (a) Employees in a specialty assignment who have fulfilled their three (3) year commitment are eligible to be selected for another specialty.
 - 5. If an employee/supervisor who is currently in a specialty unit has reached the recommended rotation time, the incumbent may remain in the assignment, based on the needs of the department as decided by the Chief of Police or designee.
 - 6. The Chief of Police maintains the right to exempt, extend or assign personnel wherever he/she feels is appropriate and/or necessary for both the needs of the department and/or employee(s).
- (b) Any employee/supervisor who is transferred out of a specialty unit because of poor performance will not be eligible for another specialized unit until the full three (3) year minimum commitment from the date of placement period has passed.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Employee/Supervisor Specialty Assignments and Rotations

1011.2.1 FULL-TIME AND PART-TIME SPECIALTIES

- (a) Full-Time Specialty - A lateral transfer to a specialty unit such as: Investigations Division, Community Resource Division, Police Service Dog (K-9) Unit, Traffic Unit, or other specialty designated by the Chief Police, which requires the attention of a full-time employee.
- (b) Part-Time Specialty - A specialty unit that is on call, seasonal, or is work in addition to an officer's full-time duties and responsibilities.
- (c) Employees of the South Salt Lake City Police Department will be limited to one (1) full-time specialty, and preferably no more than two (2) part-time specialties concurrently.
- (d) Supervisors of a specialty unit will have an opportunity to participate in the selection process.
- (e) Part-Time and Full-Time specialties will follow the three (3) year commitment and five (5) year recommended rotation policy.
- (f) Any Assignment designated as a specialty or specialized assignment shall have a selection process.

1011.3 DESK OFFICER POSITION

- (a) The desk officer position is a fixed post at the police department.
 - 1. The assignment may be made, as the needs of the department require.
 - 2. The assignment may be for an entire shift or portion of that shift as determined by the shift supervisor.
 - 3. The desk officer will assist citizens who walk into the fixed post and provide information over the telephone, by either resolving a service request or by directing the citizen to the appropriate department or personnel.
 - 4. When the desk officer determines an officer's response to the scene is appropriate, the officer will forward the information to VECC as soon as practical.
 - 5. Desk officers may be assigned other duties based on their capabilities.
- (b) If a caller is unwilling to provide the report details over the phone, or respond to the office, the desk officer should refer the incident to the shift supervisor.
- (c) When a desk officer takes a report that requires an on-scene action, such as collection of evidence, photographs, or follow-up, the desk officer will notify the on-duty supervisor as soon as practical, of the need for a patrol officer.
- (d) The desk officer will complete supplemental reports to any original report as required.
- (e) All reports shall be completed by the end of the shift, prior to going off duty. If an exception is needed, the desk officer must get approval from the shift supervisor.

Commendations and Awards

1012.1 PURPOSE AND SCOPE

This policy provides general guidelines for recognizing commendable or meritorious acts of members of the South Salt Lake Police Department and individuals from the community.

1012.2 POLICY

It is the policy of the South Salt Lake Police Department to recognize and acknowledge exceptional individual or group achievements, performance, proficiency, heroism and service of its members and individuals from the community through commendations and awards.

1012.3 COMMENDATIONS

Commendations for members of the Department or for individuals from the community may be initiated by any department member or by any person from the community.

1012.4 CRITERIA

A meritorious or commendable act may include, but is not limited to:

- Superior handling of a difficult situation.
- Conspicuous bravery or outstanding performance.
- Any action or performance that is above and beyond typical duties.

1012.4.1 DEPARTMENT MEMBER DOCUMENTATION

Members of the Department should document meritorious or commendable acts. The documentation should contain:

- (a) Identifying information:
 1. For members of the Department - name, division and assignment at the date and time of the meritorious or commendable act
 2. For individuals from the community - name, address, telephone number
- (b) A brief account of the meritorious or commendable act with report numbers, as appropriate.
- (c) The signature of the member submitting the documentation.

1012.4.2 COMMUNITY MEMBER DOCUMENTATION

Documentation of a meritorious or commendable act submitted by a person from the community should be accepted in any form. However, written documentation is preferred. Department members accepting the documentation should attempt to obtain detailed information regarding the matter, including:

- (a) Identifying information:
 1. For members of the Department - name, division and assignment at the date and time of the meritorious or commendable act

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Commendations and Awards

2. For individuals from the community - name, address, telephone number
- (b) A brief account of the meritorious or commendable act with report numbers, as appropriate.
- (c) The signature of the person submitting the documentation.

1012.4.3 PROCESSING DOCUMENTATION

Documentation regarding the meritorious or commendable act of a member of the Department should be forwarded to the appropriate Division Commander for his/her review. The Division Commander should sign and forward the documentation to the Chief of Police for his/her review.

The Chief of Police or the authorized designee will present the commendation to the department member for his/her signature. The documentation will then be returned to the Administration secretary for entry into the member's personnel file.

Documentation regarding the meritorious or commendable act of an individual from the community should be forwarded to the Administration Division Commander. The documentation will be signed by the Division Commander and forwarded to the Chief of Police for his/her review. An appropriate venue or ceremony to acknowledge the individual's actions should be arranged. Documentation of the commendation shall be maintained in a file designated for such records.

1012.5 AWARDS

Awards may be bestowed upon members of the Department and individuals from the community. These awards include:

- Award of Merit.
- Award of Valor.
- Lifesaving Award.
- Meritorious Conduct.

Criteria for each award and the selection, presentation and display of any award are determined by the Chief of Police.

Fitness for Duty

1013.1 PURPOSE AND SCOPE

Monitoring members' fitness for duty is essential for the safety and welfare of the members of the [Department/Office] and the community. The purpose of this policy is to ensure that all members of this [department/office] remain fit for duty and able to perform their job functions.

1013.2 POLICY

The South Salt Lake Police Department strives to provide a safe and productive work environment and ensure that all members of this [department/office] can safely and effectively perform the essential functions of their jobs. Under limited circumstances, the [Department/Office] may require a professional evaluation of a member's physical and/or mental capabilities to determine the member's ability to perform essential functions.

1013.3 MEMBER RESPONSIBILITIES

It is the responsibility of each member of this [department/office] to maintain physical stamina and psychological stability sufficient to safely and effectively perform essential duties of their position.

During working hours, all members are required to be alert, attentive, and capable of performing their assigned responsibilities.

Any member who feels unable to perform their duties shall promptly notify a supervisor. In the event that a member believes that another [department/office] member is unable to perform their duties, such observations and/or belief shall be promptly reported to a supervisor.

1013.4 SUPERVISOR RESPONSIBILITIES

- (a) A supervisor observing an employee or receiving a report of an employee who is perceived to be unable to safely perform their duties due to a physical or mental condition shall take prompt and appropriate action in an effort to resolve the situation.
- (b) Whenever feasible, the supervisor should attempt to ascertain the reason or source of the problem, and in all cases a preliminary evaluation should be made in an effort to determine the level of inability of the employee to perform their duties.
- (c) In the event the employee appears to be in need of immediate medical or psychiatric treatment, all reasonable efforts should be made to provide such care.
- (d) In conjunction with the Watch Commander or employee's available Division Commander, a determination should be made whether the employee should be temporarily relieved from their duties.
- (e) The Chief of Police and any other supervisor who is made aware that an officer may have a physical or mental disability affecting the officer's ability to perform their duties shall investigate the allegation (Utah Code 53-6-211).
- (f) The Chief of Police or a designee shall ensure that any allegation that an officer has a physical or mental disability affecting the officer's ability to perform their duties is reported to Utah Peace Officer Standards and Training (POST) within 30 days if the

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Fitness for Duty

allegation is substantiated (UAC R728-409-18). This applies even in those instances where an employee resigns or is terminated (Utah Code 53-6-211).

- (g) The Chief of Police shall be promptly notified in the event that any employee is relieved from duty.

1013.5 NON-WORK-RELATED CONDITIONS

Any employee suffering from a non-work-related condition which warrants a temporary relief from duty may be required to use sick leave or other paid time off (PTO) in order to obtain medical treatment or other care.

1013.6 WORK-RELATED CONDITIONS

Any employee suffering from a work-related condition which warrants a temporary relief from duty shall be required to comply with personnel rules and guidelines for processing such claims.

Upon the recommendation of the Watch Commander or unit supervisor and concurrence of a Division Commander, any employee whose actions or use of force in an official capacity result in death or serious injury to another may be temporarily removed from regularly assigned duties and/or placed on paid administrative leave for the well being of the employee and until such time as the following may be completed:

- (a) A preliminary determination that the employee's conduct appears to be in compliance with related policies.
- (b) The employee has had the opportunity to receive necessary counseling and/or psychological clearance to return to full duty.

1013.7 FITNESS FOR DUTY EVALUATIONS

Fitness for duty medical evaluations may be performed under any of the following circumstances:

- (a) Return to work from injury or illness.
- (b) When a supervisor determines there is a direct threat to the health or safety of the employee or others.
- (c) In conjunction with corrective action, performance or conduct issues or discipline.
- (d) When it is a bona fide occupational qualification for selection, retention or promotion.

1013.8 LIMITATION ON HOURS WORKED

Absent emergency operations, members should not work more than:

- 16 hours in a one-day (24 hours) period
- 30 hours in any two-day (48 hours) period
- 84 hours in any seven-day (168 hours) period

Except in unusual circumstances, members should have a minimum of eight hours off between shifts. Supervisors should give consideration to reasonable rest periods and are authorized to deny overtime or relieve any member who has exceeded the above guidelines to off-duty status.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Fitness for Duty

Limitations on the number of hours worked apply to shift changes, shift trades, rotation, holdover, training, general overtime, and any other work assignments, to include approved outside employment.

1013.9 REQUIRED EXAMINATIONS

Any physical, medical, or psychological examinations required by the [Department/Office] shall be provided at no cost to the [department/office] member.

1013.10 APPEALS

An employee who is separated from paid employment or receives a reduction in salary resulting from a fitness for duty exam shall be entitled to an administrative appeal as outlined in the Personnel Complaints Policy.

Meal Periods and Breaks

1014.1 PURPOSE AND SCOPE

This policy outlines the requirements regarding meals and breaks.

1014.1.1 MEAL PERIODS

Sworn employees shall remain on-duty subject to call out during meal breaks. All other employees are not on-call during meal breaks unless directed otherwise by a supervisor.

Uniformed patrol and traffic officers shall request clearance from Dispatch prior to taking a meal period. Uniformed officers shall take their breaks within the City limits unless on assignment outside of the City or with the approval of a supervisor.

No more than two uniformed officers or marked patrol vehicles will be authorized to take a meal break or a break at one time. Exception is given to Field Training Officers with a recruit, and will be limited to no more than three officers and two marked patrol vehicles.

Uniformed officer is any employee wearing a uniform. IE; Patrol Officer, Detective, Support Staff Officers/employees working 5 hours or less in duration are not authorized to take a meal break.

Non-sworn employees are entitled to a 30 minute uninterrupted lunch period, unless on-call or redirected by their supervisor.

All on-duty officers shall maintain radio contact with dispatch during any meal break or breaks.

Under normal circumstances, an employee may take a 30 minute meal break during each shift worked. On-duty patrol officers are encouraged to take their meal break within their assigned Community Zone if possible. Meal breaks outside of South Salt Lake City will only occur with supervisor approval.

The time spent for the meal period shall not exceed the authorized time allowed.

1014.1.2 BREAKS

Each employee is entitled to a 15-minute break, near the mid-point, for each four-hour work period (UAC R477-8-3). Only one 15-minute break shall be taken during each 4-hours of duty. No breaks shall be taken during the first or last hour of an employee's shift unless approved by a supervisor.

Employees normally assigned to the police facility shall remain in the police facility for their breaks. This would not prohibit them from taking a break outside the facility if on official business.

Field officers will take their breaks in their assigned areas, subject to call, and shall monitor their radios. When field officers take their breaks away from their vehicles, they shall do so only with the knowledge and clearance of Dispatch.

Lactation Breaks

1015.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance regarding reasonable accommodations for lactating members.

1015.2 POLICY

It is the policy of the South Salt Lake Police Department to provide, in compliance with federal and state law, reasonable accommodations for lactating members. This includes break time and appropriate facilities to accommodate any member desiring to express breast milk for the member's nursing child for up to one year after the child's birth (29 USC § 218d; 42 USC § 2000gg-1; 29 CFR 1636.3; Utah Code 34-49-203).

1015.3 LACTATION BREAK TIME

A rest period should be permitted each time the member requires a lactation break (29 USC § 218d; 42 USC § 2000gg-1; 29 CFR 1636.3; Utah Code 34-49-202). In general, lactation breaks that cumulatively total 30 minutes or less during any four-hour work period or major portion of a four-hour work period would be considered reasonable. However, individual circumstances may require more or less time.

Lactation breaks, if feasible, should be taken at the same time as the member's regularly scheduled rest or meal periods.

While a reasonable effort will be made to provide additional time beyond authorized breaks, any such time exceeding regularly scheduled and paid break time will be unpaid.

Members desiring to take a lactation break shall notify the dispatcher or a supervisor prior to taking such a break. Such breaks may be reasonably delayed if they would seriously disrupt [department/office] operations.

Once a lactation break has been approved, the break should not be interrupted except for emergency or exigent circumstances.

1015.3.1 PRESENCE OF CHILDREN

The [Department/Office] is not required to allow the child of the member to be present at the [Department/Office] for purposes of accommodating breastfeeding (Utah Code 34A-5-106).

1015.4 PRIVATE LOCATION

The [Department/Office] will make reasonable efforts to accommodate members with the use of an appropriate room or other location to express milk in private. Such room or place should be in proximity to the member's work area and shall be other than a bathroom or toilet stall. The location must have an electrical outlet and be shielded from view, free from intrusion from coworkers and the public, and otherwise satisfy the requirements of federal and state law (29 USC § 218d; 42 USC § 2000gg-1; 29 CFR 1636.3; Utah Code 34-49-202).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Lactation Breaks

Members occupying such private areas shall either secure the door or otherwise make it clear to others that the area is occupied with a need for privacy. All other members should avoid interrupting a member during an authorized break, except to announce an emergency or other urgent circumstance.

Authorized lactation breaks for members assigned to the field may be taken at the nearest appropriate private area.

1015.5 STORAGE OF EXPRESSED MILK

The [Department/Office] will provide access to a clean and well-maintained refrigerator, freezer, or other suitable container for the temporary storage of breast milk (Utah Code 34-49-202).

Any member storing expressed milk in any authorized refrigerated area within the [Department/Office] shall clearly label it as such and shall remove it when the member's shift ends.

Payroll Records

1016.1 PURPOSE AND SCOPE

This policy provides the guidelines for completing and submitting payroll records of department members who are eligible for the payment of wages.

1016.2 POLICY

The South Salt Lake Police Department maintains timely and accurate payroll records.

1016.3 RESPONSIBILITIES

Members are responsible for the accurate completion and timely submission of their payroll records for the payment of wages.

Supervisors are responsible for approving the payroll records for those under their commands.

1016.4 TIME REQUIREMENTS

Members who are eligible for the payment of wages are paid on a scheduled, periodic basis, generally on the same day or date each period, with certain exceptions, such as holidays. Payroll records shall be completed and submitted to Administration as established by the City payroll procedures.

1016.5 RECORDS

The Administration Division Commander or designee shall ensure that accurate and timely payroll records are maintained as required by 29 CFR 516.2 for a minimum of three years (29 CFR 516.5).

Overtime Compensation Requests

1017.1 PURPOSE AND SCOPE

The City will pay at least minimum wages and overtime to all employees except those who are specifically exempt from minimum wage and overtime requirements under the Fair Labor Standards Act (FLSA) of 1938. The City will also provide equal pay to all employees doing similar work which requires substantially equal skill, effort, responsibility, and performed under similar working conditions, in accordance with the Fair Labor Standards Act of 1938 and the Equal Pay Act of 1963.

1017.2 DEFINITIONS

Full-time: Employees hired for an indefinite period in a position for which the normal work schedule is forty (40) hours per week. Full-time employees may or may not qualify for specific City benefits and/or be members of the merit personnel system.

Part-time: Employees hired for an indefinite period in a position for which the normal work schedule is less than forty (40) hours per week. Part-time employees may or may not qualify for specific City benefits and/or be members of the merit personnel system. Unless otherwise specified, part-time employees must be scheduled and work at least (20) hours per week in order for the part-time position to be considered or designated as a benefited part-time position.

Temporary/Seasonal: Employees hired for a position which is required for only a specific, known duration, usually less than six (6) months. Temporary/seasonal employees may or may not qualify for specific City benefits and/or be members of the merit personnel system.

Non-exempt employees: These employees are subject to the FLSA's overtime and minimum wage requirements. They are typically paid hourly and perform more manual or technical tasks. Non-exempt employees must be paid overtime at a rate of time-and-one-half for every hour worked over 40 in a work week. They must also earn at least the federal minimum hourly wage

Exempt Employees: Exempt employees are paid a salary rather than by the hour, and they work in professional, administrative, executive, outside sales, and computer-related fields.

Fair Labor Standards Act (FLSA): The Fair Labor Standards Act (FLSA) covers all public employees, including law enforcement, unless they are specifically exempt.

To qualify for exemption, employees must meet certain job duty tests and be paid a salary

Flex Time: Flex Time accounts for a regular, non-overtime schedule and taken off during the same pay period.

Compensatory Time: Compensatory time may be earned in lieu of overtime at the same rate.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Overtime Compensation Requests

1017.3 POLICY

It is the policy of the Department to compensate non-exempt salaried employees who work authorized overtime by payment of wages. The employee must complete and submit a Request for Overtime Payment Form as soon as practical after overtime is approved and worked.

1017.4 DEPARTMENT GUIDELINE

For employees engaged in public safety activities within the Police Department: overtime pay would apply for over eighty (80) hours worked period consisting of fourteen (14) consecutive days, and shall be compensated at the rate of one and one-half (1 and 1/2) times the regular hourly rate of the employee.

If a holiday, vacation, or sick day falls within the eighty (80) hours pay period. The sworn public safety employee must work over and above these hours before overtime must be paid.

For employees not engaged in public safety activities: overtime pay would apply for over forty (40) hours worked in a work week, and shall be compensated at the rate of one and one-half (1 and 1/2) times the regular hourly rate of the employee.

If a holiday, vacation, or sick day falls within a work week, the employee must work forty (40) hours over and above these hours before overtime must be paid. If employees work on a holiday because of an emergency situation, they will receive their regular straight-time pay for the time worked, plus holiday pay.

Overtime shall be approved by the Department Head or designee, before worked. In case of emergency conditions, overtime compensation may be authorized after the work has been performed. Violation of this policy may result in disciplinary action, up to and including termination.

Non-exempt employees are not authorized to volunteer work time to the Department. All requests to work overtime shall be approved in advance by a supervisor. If circumstances do not permit prior approval, then approval shall be sought as soon as practical during the overtime shift, and in no case later than the end of shift in which the overtime is worked.

Short periods of work at the end of the normal duty day (e.g., less than one-hour in duration) may be handled unofficially between the supervisor and the employee by flexing a subsequent shift schedule to compensate for the time worked rather than by submitting requests for overtime payments. If the supervisor authorizes or directs the employee to complete a form for such a period, the employee shall comply.

1017.5 REQUEST FOR OVERTIME COMPENSATION

Employees shall submit all overtime compensation requests to their immediate supervisors as soon as practicable for verification and forwarding to the Administration Division. Failure to submit a request for overtime compensation in a timely manner (prior to payroll submission) may result in waiting to receive earned payment and discipline.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Overtime Compensation Requests

1017.5.1 EMPLOYEE'S RESPONSIBILITY

Employees shall complete the request immediately after working the overtime and turn the request in to the immediate supervisor or the Watch Commander. Employees submitting overtime cards for on-call pay when off-duty shall submit cards to their immediate supervisor. The payroll processing program is available on your phone and web based.

1017.5.2 SUPERVISOR'S RESPONSIBILITY

The supervisor who verifies the overtime earned shall verify that the overtime was worked before approving the request.

After the entry has been made on the employee's time card, the Overtime Payment Request Form is forwarded to the employee's Division Commander for final approval.

1017.5.3 DIVISION COMMANDER'S RESPONSIBILITY

Division Commanders, after approving payment, will then forward the form to the Chief of Police for review.

1017.5.4 COMPENSATORY TIME FOR NON-EXEMPT EMPLOYEES

1017.5.4 COMPENSATORY TIME FOR NON-EXEMPT EMPLOYEES

1) Compensatory time for non-exempt employees may be earned in lieu of overtime and at a rate of one and one-half hours for every hour worked over 80 hours in a pay period cycle.. Non-exempt employees engaged in public safety activities within the Police Department, may earn compensatory time in lieu of overtime when they work more than 80 hours in a 14-day work cycle. Employees selecting compensatory time in lieu of overtime pay may not accrue more than 80 hours of compensatory time at any time. When calculating compensatory time accrual, any leave, including sick leave and vacation leave, on-call time, and holiday time may not be counted as hours worked. Additionally, sick leave and vacation leave may not be used if use of such leave would result in accrual of compensatory time.

2) At any time, and in the department's sole discretion, the department may freely substitute monetary payments in whole or in part in place of compensatory time. Payments for already accrued compensatory time will be paid at the regular rate earned by the employee at the time the employee receives payment. Hours accrued in excess of the 80-hour maximum limit shall be compensated with a monetary payment to be paid in the same pay-period in which the compensatory time is earned. For hours accrued in excess of the 80-hour maximum limit, hours shall be paid at one and one-half times the employee's regular hourly rate instead of accrued.

Use of compensatory time.

3) An employee who has accrued compensatory time and makes a request to use that time must be permitted to use the time off within a reasonable period after making the request. The employee's request for use of compensatory time may be denied if it will unduly disrupt the department's operations. The employee's supervisor may require the employee to use accrued compensatory time to avoid excessive accruals.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Overtime Compensation Requests

4) All accrual of compensatory time, requests or orders to use compensatory time, and use of compensatory time shall be appropriately documented and verified by the supervisor, division commander, and Chief of Police consistent with department policies.

5) Compensatory time accrued after the effective date of this section shall be exhausted prior to the use of any other accrued time off such as sick and vacation accruals.

1017.6 EXEMPT DUTY LIEUTENANT

When a Duty Lieutenant/Watch Commander has approved time off and coverage is needed, any exempt lieutenant may cover for a duty lieutenant/watch commander. The approved assigned lieutenant shall accurately put the time worked on their time card. A note should be added. Differential pay will be authorized for Friday/Saturday/Sunday shifts from 1400-0000 or 1600-0200 only. The weekend shift cannot be flexed or modified, if differential pay is the chosen as method of compensation. If compensatory time is selected, no more that 80 hours can be accrued. Compensatory time must be utilized prior to sick or vacation accrued leave. **An FLSA-exempt employee must use accrued compensatory time off by the end of the 26th pay period after the pay period during which it was earned.**

1017.7 ACCOUNTING FOR OVERTIME WORKED

Employees are to record the actual time worked in an overtime status. The case report and a circumstance note should be added in the date note section.

1017.7.1 ACCOUNTING FOR PORTIONS OF AN HOUR

When accounting for less than a full hour, time worked shall be rounded up to the nearest quarter of an hour as illustrated below:

- 1 to 15 minutes worked - Indicate .25 hour on card
- 16 to 30 minutes worked - Indicate .50 hour on card
- 31 to 45 minutes worked - Indicate .75 hour on card
- 46 to 60 minutes worked - Indicate 1.0 hour on card

1017.7.2 VARIATION IN TIME REPORTED

Where two or more employees are assigned to the same activity, case or court trial, and the amount of time for which payment is requested varies from that reported by the other officer, the Watch Commander or other approving supervisor may require each employee to include the reason for the variation. There is a note section in the time keeping program to document discrepancies.

Outside Employment

1018.1 PURPOSE AND SCOPE

This policy sets forth rules governing outside employment in an effort to avoid actual or perceived conflicts of interest. Outside employment shall be at the discretion of the Chief of Police in accordance with the provisions of this policy and Utah Code 53-13-114.

1018.1.1 DEFINITIONS

Outside Employment - Any employee of the Department who receives wages, compensation or other consideration of value from another employer, organization or individual not affiliated directly with this department for services, product(s) or benefits rendered; for purposes of this section, the definition includes those employees who are self-employed and not affiliated directly with this department for services, product(s) or benefits rendered. Outside employment does not include volunteer, charitable, or religious work.

Law Enforcement Related Outside Employment: Outside employment that is conditioned on the actual or potential use of law enforcement powers by the police officer (employee).

Non-Law Enforcement Related Outside Employment: Outside employment that will NOT require the use or potential use of law enforcement powers.

1018.2 OBTAINING APPROVAL

No employee of the Department may engage in outside employment without first obtaining prior written approval and review of pertinent policies through the Chief of Police or designee. Failure to obtain prior written approval for outside employment or engaging in outside employment prohibited by this policy may lead to disciplinary action.

Employees who have not satisfactorily completed their initial field training, or on administrative leave, or who are on medical leave of any kind or are on light duty status are not permitted to engage in outside employment.

In order to obtain approval for related outside employment, the employee must provide a written request by completing the "Request for Outside Employment" and submitting the request to employee's direct supervisor, at least 7 days prior to the proposed start date of the law enforcement related outside employment. The application will be presented to the Chief of Police for consideration.

If approved, the employee will be provided a written documentation of the approval. Unless otherwise indicated in writing on the approval documentation the approval will be valid for a term of one year from the date of application, subject to the terms of this policy. Employees are responsible for tracking the expiration date of their related outside employment approval.

Any employee seeking approval of related outside employment, whose request has been denied, shall be provided with a written reason for the denial of the application at the time of the denial.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Outside Employment

1018.2.1 APPEAL OF DENIAL OF OUTSIDE EMPLOYMENT

If a decision is made to deny, suspend, or revoke an employee's outside employment request, the employee may file written notice of appeal within 10 days of the date of the denial and submit to the Chief's office.

1018.2.2 REVOCATION/SUSPENSION OF OUTSIDE EMPLOYMENT APPROVAL

Any outside employment approval may be revoked or suspended under the following circumstances:

- (a) Decline in employee's performance to an unsatisfactory level or overall level of competency.
- (b) As a term or condition of sustained discipline.
- (c) Employee's conduct or outside employment conflicts with the provisions of Department policy, the permit may be suspended or revoked.
- (d) When an employee is unable to perform at a full-duty capacity due to an injury or other condition or circumstance.
- (e) Any violation of the terms of this policy.

1018.3 PROHIBITED OUTSIDE EMPLOYMENT

The Department expressly reserves the right to deny any Outside Employment Application submitted by an employee seeking to engage in any activity which:

- (a) Interferes with an employee's efficiency performance.
- (b) Conflicts with the interests of the Department or the State of Utah.
- (c) Gives reason for criticism or suspicion of conflicting interests or duties.

No employee may enter into a contract to serve as a broker to provide outside employment.

Outside employment that constitutes a threat to the status or dignity of a police officers as professional occupation will not be approved. This includes but is not limited to, employment in establishments which sell pornographic books, magazines, sexual devices or videos, or that otherwise provide entertainment or services or a sexual nature; employment in establishments involving the sale of alcohol for on-site consumption, manufacture or transportation of alcohol.

No employee may engage in outside employment with any business or entity that:

- (a) Does not comply with State and Federal income reporting and withholding requirements regarding the employee's wages;
- (b) that requires the employee to disclose confidential information obtained by reason of their employment with the Department; or
- (c) restricts or interferes with the employee's ability to perform duties required of a sworn peace officer or respond to a law enforcement emergency.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Outside Employment

1018.3.1 OUTSIDE SECURITY AND PEACE OFFICER EMPLOYMENT

No employee shall engage in outside employment outside the corporate limits of the City of South Salt Lake, unless the employment is pursuant to a current agreement between the City and the employing entity..

1018.4 RULES GOVERNING OUTSIDE EMPLOYMENT

Employees engaged in outside employment shall not schedule shifts that would conflict or interfere with the employee's regularly assigned shift with the Department.

An employee engaged in outside related employment is subject to call-out in case of emergency, and is expected to leave their outside employment in such situations.

An employee engaged in any outside employment is subject to all rules, regulations, policy and procedures of the City of South Salt Lake and the South Salt Lake Police Department.

Employees may work a maximum of twenty-four (24) hours of outside employment, or a total of sixty-four (64) hours in combination with their regular duty in each week, beginning on Saturday at 0600 hours. _

Employees may not use City property, including but not limited to, vehicles, laptops, police uniforms bearing the Department's logo, when engaged in non-law enforcement related outside employment, unless working in South Salt Lake City. The use of City property for law enforcement related employment is permitted when such employment is within the jurisdictional boundaries of the City of South Salt Lake or when such use is authorized pursuant to the Department's written contract with the outside law enforcement related employer outside the City's jurisdictional boundaries.

Employees are prohibited from scheduling more than one outside employment shift during the same time period and date.

Employees are required to utilize BWC and activate per policy during department approved outside employment.

Employees are prohibited from testify in a civil cases unless legally summoned or subpoenaed. Employees shall not serve civil processes while on duty or in uniform, except those initiated by a lawful court order.

For approved law enforcement related outside employment the use of department issued vehicle is authorized to use.

For non-law enforcement related outside employment the use of department issued vehicle is unauthorized to use, unless the employment resides in South Salt Lake City, Utah.

1018.5 DUTY TO NOTIFY

If an employee arrives at an outside employment assignment and finds that fulfilling the assignment will violate this policy or any Department or City policy, they will immediately notify the on-duty Lieutenant. Employees of the department will immediately report in writing, any incident

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Outside Employment

or situations arising from or connected with their outside employment which might adversely affect the department or its personnel. All notifications will be directed to the Chief of Police through the chain of command.

In the event of the necessity to make an arrest during an outside employment assignment while working in plain clothes, the officer must call for a uniformed officer whenever possible prior to intervening. If enforcement action is required, the officer must identify themselves as law enforcement by visual and verbal means.

1018.6 OUTSIDE EMPLOYMENT RELATIONSHIP

Outside employment assignments will be determined by agreement between the outside employer and the requesting employee.

Employees working any outside employment are responsible for paying all appropriate taxes and reporting all income to the Internal Revenue Service, pursuant to the I.R.S. regulations.

The City of South Salt Lake and/or the Department are not responsible for payment conflicts, or lack of payment between the employee and the outside employer.

Officers approved to perform Law Enforcement Related Outside Employment within the jurisdictional boundaries, subject to the provisions set forth below, will be covered by benefits established under the workers compensation act and injured employee salary continuation plan, if it is determined that the officer was in the course and scope of police duties.

For the purpose of this policy, course and scope of law enforcement related duties will include:

- (a) Incidents where an officer is injured while in the act of enforcing a federal law, state law, or an ordinance of the City of South Salt Lake.
- (b) Incidents where an officer is injured solely because of their representation as a law enforcement officer or member of the South Salt Lake City Police Department.

1018.7 VIOLATIONS / GROUNDS FOR DISCIPLINARY ACTION

One or more violations of this policy may result in discipline up to, and including, termination.

1018.8 OUTSIDE EMPLOYMENT REQUEST FORM

See attachment: [Outside Employment Form.pdf](#)

Occupational Disease and Work-Related Injury and Death Reporting

1019.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance regarding the timely reporting of occupational diseases and work-related injuries and deaths.

1019.1.1 DEFINITIONS

Definitions related to this policy include:

Work-related injury or occupational disease - An accidental injury or occupational disease that arises out of and in the course of employment with the South Salt Lake Police Department. The disease must be medically caused or aggravated by that employment. An occupational disease may include a physical, mental or emotional disease related to mental stress that arises out of and in the course of employment (Utah Code 34A-3-103; Utah Code 34A-3-106; UAC R612-100-2).

1019.2 POLICY

The South Salt Lake Police Department will address occupational diseases and work-related injuries and deaths appropriately, and will comply with applicable state workers' compensation requirements (Utah Code 34A-2-407; UAC R612-200-1).

1019.3 RESPONSIBILITIES

1019.3.1 MEMBER RESPONSIBILITIES

Any member sustaining any occupational disease or work-related injury shall report such event as soon as practicable, but within 24 hours, to a supervisor, and shall seek medical care when appropriate.

1019.3.2 SUPERVISOR RESPONSIBILITIES

A supervisor learning of any occupational disease or work-related injury should ensure the member receives medical care as appropriate.

Supervisors shall ensure that required documents regarding workers' compensation are completed and forwarded promptly. Any related Citywide disease- or injury-reporting protocol shall also be followed.

Supervisors shall determine whether the Major Incident Notification and Illness and Injury Prevention policies apply and take additional action as required.

1019.3.3 DIVISION COMMANDER RESPONSIBILITIES

The Division Commander who receives a report of an occupational disease or a work-related injury or death should review the report for accuracy and determine what additional action should be taken. The report shall then be forwarded to the Chief of Police, the City's risk management entity, and the Administration Division Commander to ensure any required Utah Occupational Safety and

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Occupational Disease and Work-Related Injury and Death Reporting

Health Administration (OSHA) reporting is made as required in the injury and illness prevention plan identified in the Illness and Injury Prevention Policy.

1019.3.4 CHIEF OF POLICE RESPONSIBILITIES

The Chief of Police shall review and forward copies of the report to the Department of Human Resources. Copies of the report and related documents retained by the Department shall be filed in the member's confidential medical file.

1019.4 OTHER DISEASE OR INJURY

Diseases, injuries or deaths caused or occurring on-duty that do not qualify for workers' compensation reporting shall be documented on the designated report of injury form, which shall be signed by a supervisor. A copy of the completed form shall be forwarded to the appropriate Division Commander through the chain of command and a copy sent to the Administration Division Commander.

Unless the injury is extremely minor, this report shall be signed by the affected member, indicating that he/she desired no medical attention at the time of the report. By signing, the member does not preclude his/her ability to later seek medical attention.

1019.5 SETTLEMENT OFFERS

When a member sustains an occupational disease or work-related injury that is caused by another person and is subsequently contacted by that person, his/her agent, insurance company or attorney and offered a settlement, the member shall take no action other than to submit a written report of this contact to his/her supervisor as soon as possible.

1019.5.1 NO SETTLEMENT WITHOUT PRIOR APPROVAL

No less than 10 days prior to accepting and finalizing the settlement of any third-party claim arising out of or related to an occupational disease or work-related injury, the member shall provide the Chief of Police with written notice of the proposed terms of such settlement. In no case shall the member accept a settlement without first providing written notice to the Chief of Police. The purpose of such notice is to permit the City to determine whether the offered settlement will affect any claim the City may have regarding payment for damage to equipment or reimbursement for wages against the person who caused the disease or injury, and to protect the City's right of subrogation, while ensuring that the member's right to receive compensation is not affected.

1019.6 BENEFIT PROTECTION CONTRACT

The South Salt Lake Police Department will provide a benefit protection contract for any public safety service employee who suffers a qualifying injury or illness as defined and required in state law (Utah Code 49-14-602).

Personal Appearance Standards

1020.1 PURPOSE AND SCOPE

In order to project uniformity and neutrality toward the public and other members of the Department, it is the policy of the Department that employees shall maintain their personal hygiene and appearance to project a professional image appropriate for this department and for their assignment.

1020.2 GROOMING STANDARDS

Unless otherwise stated and because deviations from these standards could present officer safety issues, the following appearance standards shall apply to all employees, except those whose current assignment would deem them not appropriate, and where the Chief of Police has granted exception.

1020.2.1 HAIR

Hairstyles of all members shall be neat in appearance. For male sworn members, hair must not extend below the top edge of the uniform collar while assuming a normal stance.

For female sworn members, hair must be no longer than the horizontal level of the bottom of the uniform patch when the employee is standing erect. It can be worn up or in a tightly wrapped braid or ponytail.

1020.2.2 MUSTACHES

A short and neatly trimmed mustache may be worn. Mustaches shall not extend below the corners of the mouth or beyond the natural hairline of the upper lip.

1020.2.3 SIDEBURNS

Sideburns shall not extend below the bottom of the earlobe and shall be trimmed and neat.

1020.2.4 FACIAL HAIR

Traditional full beards may be worn if they are well groomed and neatly trimmed at all times in order to prevent a ragged appearance. Full Beards and goatees are authorized, but patchy, spotty clumps of facial hair are not considered beards and as such are not permitted. Full beards are defined as facial hair covering the upper lip and mouth, extending just below the cheekbones, down under the chin and jawbone, with the neck remaining clean shaven. Other variations or partial beards are prohibited.

Officers may work during a "grow-in" period; however, officers are prohibited from repeatedly starting and stopping the "grow-in" period in an effort to maintain an unshaven look. Facial hair may not be longer than 3/8 of an inch.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Personal Appearance Standards

1020.2.5 FINGERNAILS

Fingernails extending beyond the tip of the finger can pose a safety hazard to officers or others. For this reason, fingernails shall be trimmed so that no point of the nail extends beyond the tip of the finger.

1020.2.6 JEWELRY

For the purpose of this policy, jewelry refers to rings, earrings, necklaces, bracelets, wristwatches, and tie tacks or tie bars. Jewelry shall present a professional image and may not create a safety concern for the department member or others. Jewelry that depicts racial, sexual, discriminatory, gang-related, or obscene language is not allowed.

- (a) Necklaces shall not be visible above the shirt collar.
- (b) Earrings shall be small and worn only in or on the earlobe.
- (c) One ring or ring set may be worn on each hand of the department member. No rings should be of the type that would cut or pose an unreasonable safety risk to the member or others during a physical altercation, if the member is assigned to a position where that may occur.
- (d) One small bracelet, including a bracelet identifying a medical condition, may be worn on one arm.
- (e) Wristwatches shall be conservative and present a professional image.
- (f) Tie tacks or tie bars worn with civilian attire shall be conservative and present a professional image.

1020.3 TATTOOS

Tattoos, Brands, or body art which include offensive language or images, as determined by the department, or are located on the Face, Neck, Head or Hands is prohibited. Elaborate Tattoos in prominent locations and extreme hair colors or styles that loudly call attention to the employee, distract from the professionalism, propriety and decorum the public expects of those who conduct its business

Visible jewelry inserted into body piercing(s), aside from modestly pierced earlobes, is prohibited on the job.

1020.4 BODY PIERCING OR ALTERATION

Body piercing or alteration to any area of the body visible in any authorized uniform or attire that is a deviation from normal anatomical features and which is not medically required is prohibited. Such body alteration includes, but is not limited to:

- (a) Tongue splitting or piercing.
- (b) The complete or transdermal implantation of any material other than hair replacement.
- (c) Abnormal shaping of the ears, eyes, nose or teeth.
- (d) Branding or scarification.

Uniform Regulations

1021.1 PURPOSE AND SCOPE

The uniform policy of the South Salt Lake Police Department is established to ensure that uniformed officers will be readily identifiable to the public through the proper use and wearing of Department uniforms. Employees should also refer to the following associated policies:

- Department-Owned and Personal Property
- Body Armor
- Grooming Standards

The Uniform and Equipment Specifications manual is maintained and periodically updated by the Chief of Police or designee. That manual should be consulted regarding authorized equipment and uniform specifications.

The South Salt Lake Police Department will provide uniforms for all employees required to wear them in the manner, quantity and frequency agreed upon in the respective employee group's collective bargaining agreement.

1021.2 WEARING AND CONDITION OF UNIFORM AND EQUIPMENT

Police employees wear the uniform to be identified as the law enforcement authority in society. The uniform also serves an equally important purpose which is to identify the wearer as a source of assistance in an emergency, crisis or other time of need.

- (a) Uniform and equipment shall be maintained in a serviceable condition and shall be ready at all times for immediate use. Uniforms shall be neat, clean and appear professionally pressed.
- (b) All peace officers of the Department shall possess and maintain at all times a serviceable uniform and the necessary equipment to perform uniformed field duty.
- (c) Personnel shall wear only the uniform specified for their rank and assignment.
- (d) The uniform is to be worn in compliance with the specifications set forth in the Department's uniform specifications which are maintained separately from this policy.
- (e) All supervisors will perform periodic inspections of their personnel to ensure conformance to these regulations.
- (f) Civilian attire shall not be worn in combination with any distinguishable part of the uniform.
- (g) Uniforms are only to be worn while on-duty, while in transit to or from work, for court or at other official Department functions or events.
- (h) FTO trainees, If the uniform is worn while in transit, an outer garment shall be worn over the uniform shirt so as not to bring attention to the employee while he/she is off-duty.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Uniform Regulations

- (i) Employees are not to purchase or drink alcoholic beverages while wearing any part of the Department uniform including the uniform pants.
- (j) Visible jewelry, other than those items listed below, shall not be worn with the uniform unless specifically authorized by the Chief of Police or designee.
 - 1. Wrist watch.
 - 2. Wedding ring(s), class ring or other ring of tasteful design. A maximum of one ring/set may be worn on each hand.
 - 3. Medical alert bracelet.
 - 4. Female officers or professional support staff may wear small stud earrings or small hoop earrings. Professional in style.

1021.2.1 DEPARTMENT-ISSUED IDENTIFICATION

The Department issues each employee an official Department identification card bearing the employee's name, identifying information and photo likeness. All employees shall be in possession of their Department-issued identification card at all times while on-duty or when carrying a concealed weapon.

- (a) Whenever on-duty or acting in an official capacity representing the Department, employees shall display their Department-issued identification in a courteous manner to any person upon request and as soon as practical.
- (b) Officers working specialized assignments may be excused from the possession and display requirements when directed by their Division Commander.

1021.2.2 CLOTHING AND EQUIPMENT ALLOWANCE

- (a) Employees assigned to areas requiring them to wear a uniform shall receive a clothing allowance as determined by the City of South Salt Lake on an annual basis.
 - 1. Support staff will receive a clothing allowance. The annual amount and the payment schedule will be determined by the Chief of Police or his/her designee.
 - 2. Sworn personnel and approved support staff will be issued a STAR Card to purchase approved uniforms and equipment, with an annual credited amount determined by the Chief of Police each fiscal year.
 - (a) The STAR Card is an individually credited account established at SKAGGS Public Safety Uniforms & Equipment, a supplier in the City of South Salt Lake for sworn and non-sworn personnel to purchase needed uniforms and equipment related to their current police assignments at the South Salt Lake Police Department.
 - 1. A "Purchasing Profile" will be created at SKAGGS, identifying all items approved for purchase.
 - 2. The STAR Card is valid for approved purchases between July 1st and May 15th each fiscal year.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Uniform Regulations

3. Any credited STAR Card funds remaining at the May 15th deadline are forfeited.
4. STAR Card purchases are prohibited if any employee has:
 - (a) Submitted a Notice of Resignation.
 - (a) Upon resignation, purchased items from the STAR car will be turned in to immediate supervisor prior to last day of employment.
 - (b) Has been placed on Administrative Leave.
 - (c) Is on Medical Leave or any approved Leave of Absence.
- (b) Supervisors are expected to monitor daily grooming and attire of personnel and can direct employees as to their cleanliness, appropriateness of attire, and overall condition of clothing.
 1. Uniforms shall include duty equipment and other related items unless otherwise designated by the Chief of Police.
 2. Required equipment and uniforms for Specialty Units shall be provided by the department with approval of the Chief of Police or his/her designee.

1021.3 UNIFORM CLASSES

1021.3.1 CLASS A UNIFORM

The Class A uniform is to be worn on special occasions, such as funerals, graduations, ceremonies or as directed. The Class A uniform is required for all sworn personnel. The Class A uniform includes the standard issue uniform with:

- (a) Long-sleeve shirt with tie.
- (b) Polished shoes.

Boots with pointed toes are not permitted.

1021.3.2 CLASS B UNIFORM

All officers will possess and maintain a serviceable Class B uniform at all times.

The Class B uniform will consist of the same garments and equipment as the Class A uniform with the following exceptions:

- (a) The long- or short-sleeve shirt may be worn with the collar open. No tie is required.
- (b) A navy blue or black crew-neck tee-shirt must be worn with the uniform.
- (c) All shirt buttons must remain buttoned except for the last button at the neck.
- (d) Shoes for the Class B uniform may be as described in the Class A uniform.
- (e) Approved all black unpolished shoes may be worn.
- (f) Boots with pointed toes are not permitted.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Uniform Regulations

1021.3.3 SPECIALIZED UNIT UNIFORMS

The Chief of Police may authorize special uniforms to be worn by officers in specialized units, such as Canine Team, SWAT, Bicycle Patrol, Motor Officers and other specialized assignments.

1021.3.4 INCLEMENT WEATHER GEAR

The Uniform and Equipment Specifications list at SKAGGS has the authorized uniform jacket and rain gear.

1021.4 INSIGNIA AND PATCHES

- (a) Shoulder Patches - The authorized shoulder patch supplied by the Department shall be machine stitched to the sleeves of all uniform shirts and jackets, 3/4-inch below the shoulder seam of the shirt, and should be bisected by the crease in the sleeve.
- (b) Service stripes and/or stars - Service stripes and other indicators for length of service may be worn on long-sleeve shirts and jackets. They are to be machine stitched onto the uniform. The bottom of the service stripe shall be sewn the width of 1-1/2 inches above the cuff seam, with the rear of the service stripes sewn-on the dress of the sleeve. The stripes are to be worn on the left sleeve only.
- (c) The regulation nameplate, or an authorized sewn-on cloth nameplate, shall be worn at all times while in uniform. The nameplate shall display the employee's first initial and last name. The nameplate shall be worn and placed above the right pocket located in the middle, bisected by the pressed shirt seam, with equal distance from both sides of the nameplate to the outer edge of the pocket.
- (d) When a jacket is worn, the nameplate or an authorized sewn-on cloth nameplate shall be affixed to the jacket in the same manner as the uniform.
- (e) Assignment Insignias - Assignment insignias (SWAT, FTO) may be worn as designated by the Chief of Police.
- (f) Flag Pin - A flag pin may be worn, centered above the nameplate.
- (g) Badge - The Department-issued badge or an authorized sewn-on cloth replica must be worn and visible at all times while in uniform.
- (h) Rank Insignia - The designated insignia indicating the employee's rank must be worn at all times while in uniform. The Chief of Police may authorize exceptions.

1021.4.1 MOURNING BADGE

Uniformed employees shall wear a black mourning band across the uniform badge whenever a law enforcement officer is killed in the line of duty. The following mourning periods will be observed:

- (a) An officer of the Department - From the time of death until midnight on the 14th day after the death.
- (b) An officer from this or an adjacent county - From the time of death until midnight on the day of the funeral.
- (c) Funeral attendee - While attending the funeral of an out-of-region fallen officer.
- (d) National Peace Officers Memorial Day (May 15) - From 0001 hours until 2359 hours.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Uniform Regulations

- (e) As directed by the Chief of Police.

1021.5 PROFESSIONAL SUPPORT ATTIRE

There are assignments within the [Department/Office] that do not require a uniform because recognition and authority are not essential to their function. There are also assignments in which the wearing of civilian attire is necessary.

- (a) All employees shall wear clothing that fits properly, is clean and free of stains, and is not damaged or excessively worn.
- (b) All male administrative, investigative, and professional support personnel who elect to wear civilian clothing to work shall wear button-style shirts with a collar and slacks or suits that are moderate in style.
- (c) All female administrative, investigative, and professional support personnel who elect to wear civilian clothes to work shall wear dresses, slacks, shirts, blouses, or suits that are moderate in style.
- (d) Sworn officers in investigations that choose to wear civilian attire shall wear their badge around the neck, to more readily identify themselves as officers.
- (e) The following items shall not be worn on-duty:
 - 1. T-shirt alone.
 - 2. Thong sandals/flip flops.
 - 3. Swimsuit, tube tops, or halter-tops.
 - 4. Spandex-type pants or see-through clothing.
 - 5. Distasteful printed slogans, buttons, or pins.
- (f) Variations from this order are allowed at the discretion of the Chief of Police or designee when the employee's assignment or current task is not conducive to the wearing of such clothing.
- (g) No item of professional attire may be worn on-duty that would adversely affect the reputation of the South Salt Lake Police Department or the morale of the employees.
- (h) Any uniform worn by a civilian employee shall be clearly distinguishable from that of a regular officer. Tan utility pants and black shirts are not authorized wear for civilian uniform.
- (i) All professional support staff is authorized to wear Jean style pants on Fridays only. Jeans may not have holes or rips in them.
- (j) All professional support staff will receive a STAR card to purchase approved South Salt Lake Police Logo items and work wear.

1021.6 POLITICAL ACTIVITIES, ENDORSEMENTS, AND ADVERTISEMENTS

Unless specifically authorized by the Chief of Police, South Salt Lake Police Department employees may not wear any part of the uniform, be photographed wearing any part of the uniform, utilize a Department badge, patch or other official insignia, or cause to be posted, published or

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Uniform Regulations

displayed, the image of another employee, or identify himself/herself as an employee of the South Salt Lake Police Department to do any of the following:

- (a) Endorse, support, oppose or contradict any political campaign or initiative.
- (b) Endorse, support, oppose or contradict any social issue, cause or religion.
- (c) Endorse, support or oppose any product, service, company or other commercial entity.
- (d) Appear in any commercial, social or non-profit publication, or any motion picture, film, video, public broadcast or any Web site.

1021.7 OPTIONAL EQUIPMENT - MAINTENANCE AND REPLACEMENT

- (a) Any of the items listed in the Uniform and Equipment Specifications as optional shall be purchased totally at the expense of the employee. No part of the purchase cost shall be offset by the Department for the cost of providing the Department-issued item.
- (b) Maintenance of optional items shall be the financial responsibility of the purchasing employee. For example, repairs due to normal wear and tear.
- (c) Replacement of items listed in this order as optional shall be done as follows:
 - 1. When the item is no longer functional because of normal wear and tear, the employee bears the full cost of replacement.
 - 2. When the item is no longer functional because of damage in the course of the employee's duties, it shall be replaced following the procedures for the replacement of damaged personal property outlined in the Department-Owned and Personal Property Policy.

1021.8 UNAUTHORIZED UNIFORMS, EQUIPMENT AND ACCESSORIES

South Salt Lake Police Department employees may not wear any uniform item, accessory or attachment unless specifically authorized in the Uniform and Equipment Specifications or by the Chief of Police or designee.

South Salt Lake Police Department employees may not use or carry any safety item, tool or other piece of equipment unless specifically authorized in the Uniform and Equipment Specifications or by the Chief of Police or designee.

Nepotism and Conflicting Relationships

1022.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure equal opportunity and effective employment practices by avoiding actual or perceived favoritism, discrimination or other actual or potential conflicts of interest by or between members of the Department. These employment practices include: recruiting, testing, hiring, compensation, assignment, use of facilities, access to training opportunities, supervision, performance appraisal, discipline and workplace safety and security.

1022.1.1 DEFINITIONS

Definitions related to this policy include:

Appointee - An employee whose salary, wages, pay, or compensation is paid from public funds (Utah Code 52-3-1).

Business relationship - Serving as an employee, independent contractor, compensated consultant, owner, board member, shareholder, or investor in an outside business, company, partnership, corporation, venture, or other transaction where the Department employee's annual interest, compensation, investment, or obligation is greater than \$250.

Conflict of interest - Any actual, perceived, or potential conflict of interest in which it reasonably appears that a Department employee's action, inaction, or decisions are or may be influenced by the employee's personal or business relationship.

Household member - A person who resides in the same residence as the public officer (Utah Code 52-3-1).

Nepotism - The practice of showing favoritism to relatives in appointment, employment, promotion, or advancement by any public official in a position to influence these personnel decisions.

Personal relationship - Includes marriage, cohabitation, dating, or any other intimate relationship beyond mere friendship.

Public officer - An employee who holds a position that is compensated by public funds.

Relative - An employee's father, mother, husband, wife, son, daughter, sister, brother, grandfather, grandmother, uncle, aunt, nephew, niece, grandson, granddaughter, first cousin, mother-in-law, father-in-law, brother-in-law, sister-in-law, son-in-law, or daughter-in-law (Utah Code 52-3-1).

Subordinate - An employee who is subject to the temporary or ongoing direct or indirect authority of a supervisor.

Supervisor - An employee who has temporary or ongoing direct or indirect authority over the actions, decisions, evaluation, and/or performance of a subordinate employee.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Nepotism and Conflicting Relationships

1022.2 RESTRICTED DUTIES AND ASSIGNMENTS

The Department will not prohibit all personal or business relationships between employees. However, in order to avoid nepotism or other inappropriate conflicts, the following reasonable restrictions shall apply.

- (a) A public officer may not employ, appoint, vote for, or recommend the appointment of an appointee when the appointee will be directly supervised by a relative or a household member, unless the appointment occurs in compliance with the requirements of Utah Code 52-3-1.
- (b) Employees are prohibited from directly supervising, occupying a position in the line of supervision, or being directly supervised by any other employee who is a relative, household member, or with whom they are involved in a personal or business relationship unless the supervision occurs in compliance with the requirements of Utah Code 52-3-1.
 - 1. If circumstances require that such a supervisor/subordinate relationship exists temporarily, the supervisor shall make every reasonable effort to defer matters pertaining to the involved employee to an uninvolved supervisor.
 - 2. When personnel and circumstances permit, the Department will attempt to make every reasonable effort to avoid placing employees in such supervisor/subordinate situations. The Department, however, reserves the right to transfer or reassign any employee to another position within the same classification in order to avoid conflicts with any provision of this policy.
- (c) Employees are prohibited from participating in, contributing to, or recommending promotions, assignments, performance evaluations, transfers, or other personnel decisions affecting an employee who is a relative, household member, or with whom they are involved in a personal or business relationship.
- (d) Whenever possible, FTOs and other trainers will not be assigned to train relatives or household members. FTOs and other trainers are prohibited from entering into or maintaining personal or business relationships with any employee they are assigned to train until such time as the training has been successfully completed and the employee is off probation.
- (e) To avoid actual or perceived conflicts of interest, members of the Department shall refrain from developing or maintaining personal or financial relationships with victims, witnesses or other individuals during the course of, or as a direct result of, any official contact.
- (f) Except as required in the performance of official duties or in the case of immediate relatives, employees shall not develop or maintain personal or financial relationships with any individuals they know or reasonably should know are under criminal investigation, are convicted felons, parolees, fugitives, or registered sex offenders, or anyone who engages in serious violations of state or federal laws.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Nepotism and Conflicting Relationships

1022.2.1 EMPLOYEE RESPONSIBILITY

Prior to entering into any personal or business relationship or other circumstance which the employee knows or reasonably should know could create a conflict of interest or other violation of this policy, the employee shall promptly notify his/her uninvolvement, next highest level of supervisor.

Whenever any employee is placed in circumstances that would require the employee to take enforcement action or provide official information or services to any relative or individual with whom the employee is involved in a personal or business relationship, the employee shall promptly notify his/her uninvolvement, immediate supervisor.

In the event that no uninvolvement supervisor is immediately available, the employee shall promptly notify dispatch to have another uninvolvement employee either relieve the involved employee or minimally remain present to witness the action.

1022.2.2 SUPERVISOR'S RESPONSIBILITY

Upon being notified of, or otherwise becoming aware of any circumstance that could result in or constitute an actual or potential violation of this policy, a supervisor shall take all reasonable steps to promptly mitigate or avoid such violations whenever possible. Supervisors shall also promptly notify the Chief of Police of such actual or potential violations, through the chain of command.

Department Badges

1023.1 PURPOSE AND SCOPE

The South Salt Lake Police Department badge and uniform patch as well as the likeness of these items and the name of the South Salt Lake Police Department are property of the Department and their use shall be restricted as set forth in this policy.

1023.2 POLICY

The uniform badge shall be issued to Department members as a symbol of authority. The use and display of Department badges shall be in strict compliance with this policy. Only authorized badges issued by this department shall be displayed, carried or worn by members while on-duty or otherwise acting in an official or authorized capacity.

1023.2.1 FLAT BADGE

Sworn officers, with the written approval of the Chief of Police may purchase, at his/her own expense, a flat badge capable of being carried in a wallet. The use of the flat badge is subject to the same policies as the uniform badge.

- (a) An officer may sell, exchange or transfer the flat badge to another officer within the South Salt Lake Police Department with the written approval of the Chief of Police.
- (b) Should the flat badge become lost, damaged or otherwise removed from the officer's control, he/she shall make the proper notifications as outlined in the Department-Owned and Personal Property Policy.
- (c) An honorably retired officer may keep his/her flat badge upon retirement.
- (d) The purchase, carrying or display of a flat badge is not authorized for non-sworn personnel.

1023.2.2 CIVILIAN NON-SWORN PERSONNEL

Badges and Department identification cards issued to non-sworn personnel shall be clearly marked to reflect the position of the employee (e.g. records, victim advocate, crime analyst or crime scene investigator, evidence technician.)).

- (a) Non-sworn personnel shall not display any Department badge except as a part of required uniform and while on-duty or otherwise acting in an official and authorized capacity.
- (b) Non-sworn personnel shall not display any Department badge or represent him/herself, on- or off-duty, in such a manner which would cause a reasonable person to believe that he/she is a sworn peace officer.

1023.2.3 RETIREE UNIFORM BADGE

Upon honorable retirement employees may purchase his/her assigned duty badge for display purposes. It is intended that the duty badge be used only as private memorabilia, as other uses of the badge may be unlawful or in violation of this policy.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Department Badges

1023.3 UNAUTHORIZED USE

Except as required for on-duty use by current employees, no badge designed for carry or display in a wallet, badge case or similar holder shall be issued to anyone other than a current or honorably retired peace officer.

Department badges are issued to all sworn employees and non-sworn uniformed employees for official use only. The Department badge, shoulder patch or the likeness thereof, or the Department name shall not be used for personal or private reasons including, but not limited to, letters, memoranda and electronic communications such as electronic mail, or Web sites and Web pages.

The use of the badge, uniform patch and Department name for all material (printed matter, products or other items) developed for Department use shall be subject to approval by the Chief of Police.

Employees shall not loan his/her Department badge or identification card to others and shall not permit the badge or identification card to be reproduced or duplicated.

1023.4 PERMITTED USE BY EMPLOYEE GROUPS

The likeness of the Department badge shall not be used without the expressed authorization of the Chief of Police and shall be subject to the following:

- (a) The employee associations may use the likeness of the Department badge for merchandise and official association business provided they are used in a clear representation of the association and not the South Salt Lake Police Department. The following modifications shall be included:
 - 1. The text on the upper and lower ribbons is replaced with the name of the employee association.
 - 2. The badge number portion displays the acronym of the employee association.
- (b) The likeness of the Department badge for endorsement of political candidates shall not be used without the expressed approval of the Chief of Police.

Temporary Modified-Duty Assignments

1024.1 PURPOSE AND SCOPE

This policy establishes procedures for providing temporary modified-duty assignments. This policy is not intended to affect the rights or benefits of employees under federal or state law, City rules, or current collective bargaining agreements. For example, nothing in this policy affects the obligation of the [Department/Office] to engage in a good faith, interactive process to consider reasonable accommodations for any employee with a temporary or permanent disability or limitation that is protected under federal or state law.

1024.2 POLICY

Subject to operational considerations, the South Salt Lake Police Department may identify temporary modified-duty assignments for employees who have an injury or medical condition resulting in temporary work limitations or restrictions. A temporary assignment allows the employee to work, while providing the Department with a productive employee during the temporary period.

1024.3 GENERAL CONSIDERATIONS

Priority consideration for temporary modified-duty assignments will be given to employees with work-related injuries or illnesses that are temporary in nature. Employees having disabilities covered under the Americans with Disabilities Act (ADA) or the Utah Antidiscrimination Act (Utah Code 34A-5-101 et seq.) shall be treated equally, without regard to any preference for a work-related injury.

No position in the South Salt Lake Police Department shall be created or maintained as a temporary modified-duty assignment.

Temporary modified-duty assignments are a management prerogative and not an employee right. The availability of temporary modified-duty assignments will be determined on a case-by-case basis, consistent with the operational needs of the [Department/Office]. Temporary modified-duty assignments are subject to continuous reassessment, with consideration given to operational needs and the employee's ability to perform in a modified-duty assignment.

The Chief of Police or the authorized designee may restrict employees working in temporary modified-duty assignments from wearing a uniform, displaying a badge, carrying a firearm, operating an emergency vehicle, or engaging in outside employment, or may otherwise limit them in employing their peace officer powers.

Temporary modified-duty assignments shall generally not exceed a cumulative total of 1,040 hours in any one-year period.

1024.4 PROCEDURE

Employees may request a temporary modified-duty assignment for short-term injuries or illnesses.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Modified-Duty Assignments

Employees seeking a temporary modified-duty assignment should submit a written request to their Division Commanders or the authorized designees. The request should, as applicable, include a certification from the treating medical professional containing:

- (a) An assessment of the nature and probable duration of the illness or injury.
- (b) The prognosis for recovery.
- (c) The nature and scope of limitations and/or work restrictions.
- (d) A statement regarding any required workplace accommodations, mobility aids or medical devices.
- (e) A statement that the employee can safely perform the duties of the temporary modified-duty assignment.

The Division Commander will make a recommendation through the chain of command to the Chief of Police regarding temporary modified-duty assignments that may be available based on the needs of the Department and the limitations of the employee. The Chief of Police or the authorized designee shall confer with the Department of Human Resources or the City Attorney as appropriate.

Requests for a temporary modified-duty assignment of 20 hours or less per week may be approved and facilitated by the Watch Commander or Division Commander, with notice to the Chief of Police.

1024.4.1 ASSIGNMENT TO MODIFIED DUTY

At the direction of the Division Commander or other assigning supervisor, employees assigned to modified duty shall work the scheduled shift of the unit to which they are assigned or the shift, hours and duties specified in the modified assignment until re-assigned to another modified assignment, cleared for full duty or removed/excluded from assignment to modified duties. The Division Commander or other assigning supervisor has the discretion of re-assigning modified duty schedules to suit Department needs.

The employee and supervisors should be informed in writing of the schedule, modified duty assignment, supervisor and limitations and/or restrictions as directed by the treating physician or the Department. Such assignments will be on-site and productive in nature to the department.

See attachment: [Light Duty Form.pdf](#)

1024.4.2 ACCOUNTABILITY

Supervisors of the regular and modified duty assignments for the employee shall coordinate efforts to ensure proper time accountability. The supervisor for the modified duty assignment shall complete a change of shift/assignment form and process the form appropriately.

While on duty, employees on modified duty are responsible for coordinating required doctor visits and physical therapy in advance with their supervisor and must properly account for the time.

Employees shall immediately notify their supervisor if there is a change in their condition, which causes their physician to modify their duty assignment in any fashion and shall submit a status

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Modified-Duty Assignments

report for each visit to the treating physician. A duty status report shall be provided by employees assigned to light duty to their supervisor no less than every 30 days the employee is on modified duty.

Supervisors of employees on modified duty shall keep the Division Commander apprised of the employee's status and ability to perform the modified duty assignment. Modified duty assignments which extend beyond 60 days will require a written status report and request for extension to the Division Commander updating the history, current status and anticipated date of return to regular duty. Extensions require approval by the Chief of Police. When it is determined that an employee is no longer to perform a modified duty assignment, the supervisor of the modified duty assignment shall notify the Division Commander, documenting and coordinating the change as necessary, completing a change of shift/assignment form and process the form appropriately. All training and certification necessary for return to regular duty shall be reviewed and updated as necessary.

1024.4.3 MEDICAL EXAMINATIONS

The Department may request a medical examination by a physician retained by the Department prior to the employee's return to work and/or release to full duty. The Department may also request a medical examination by a physician retained by the Department to determine if it is appropriate for the employee to work a modified duty assignment. Such medical examinations shall be at the expense of the Department.

Employees shall return to their regularly assigned duties when they have recovered from their illness, injury or condition and the treating physician provides the Department with a signed clearance for full duty indicating that they are capable of performing the basic and essential job functions of his/her assignment.

1024.5 ACCOUNTABILITY

Written notification of assignments, work schedules and any restrictions should be provided to employees assigned to temporary modified-duty assignments and their supervisors. Those assignments and schedules may be adjusted to accommodate department operations and the employee's medical appointments, as mutually agreed upon with the Division Commander.

1024.5.1 EMPLOYEE RESPONSIBILITIES

The responsibilities of employees assigned to temporary modified duty shall include, but not be limited to:

- (a) Communicating and coordinating any required medical and physical therapy appointments in advance with their supervisors.
- (b) Promptly notifying their supervisors of any change in restrictions or limitations after each appointment with their treating medical professionals.
- (c) Communicating a status update to their supervisors no less than once every 30 days while assigned to temporary modified duty.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Modified-Duty Assignments

- (d) Submitting a written status report to the Division Commander that contains a status update and anticipated date of return to full-duty when a temporary modified-duty assignment extends beyond 60 days.

1024.5.2 SUPERVISOR RESPONSIBILITIES

The employee's immediate supervisor shall monitor and manage the work schedule of those assigned to temporary modified duty.

The responsibilities of supervisors shall include, but not be limited to:

- (a) Periodically apprising the Division Commander of the status and performance of employees assigned to temporary modified duty.
- (b) Notifying the Division Commander and ensuring that the required documentation facilitating a return to full duty is received from the employee.
- (c) Ensuring that employees returning to full duty have completed any required training and certification.

1024.6 MEDICAL EXAMINATIONS

Prior to returning to full-duty status, employees shall be required to provide certification from their treating medical professionals stating that they are medically cleared to perform the essential functions of their jobs without restrictions or limitations.

The Department may require a fitness-for-duty examination prior to returning an employee to full-duty status, in accordance with the Fitness for Duty Policy.

1024.7 PREGNANCY

If an employee is temporarily unable to perform regular duties due to a pregnancy, childbirth, or a related medical condition, the employee will be treated the same as any other temporarily disabled employee (42 USC § 2000e(k)). A pregnant employee shall not be involuntarily transferred to a temporary modified-duty assignment.

If notified by an employee or the employee's representative regarding limitations related to pregnancy, childbirth, or related medical conditions, the [Department/Office] should make reasonable efforts to provide an accommodation for the employee in accordance with federal and state law. The accommodation should be provided without unnecessary delay, as appropriate (42 USC § 2000gg-1; 29 CFR 1636.3; 29 CFR 1636.4; Utah Code 34A-5-106(1)(g)).

1024.7.1 NOTIFICATION

Pregnant employees should notify their immediate supervisors as soon as practicable and provide a statement from their medical providers identifying any pregnancy-related job restrictions or limitations. If at any point during the pregnancy it becomes necessary for the employee to take a leave of absence, such leave shall be granted in accordance with the City's personnel rules and regulations regarding family and medical care leave.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Temporary Modified-Duty Assignments

1024.8 DESK OFFICER POSITION

- (a) The desk officer position is a fixed post at the police department.
 - (a) The assignment may be made, as the needs of the department require.
 - (b) The assignment may be for an entire shift or portion of that shift as determined by the shift supervisor.
 - (c) The desk officer will assist citizens who walk into the fixed post and provide information over the telephone, by either resolving a service request or by directing the citizen to the appropriate department or personnel.
 - (d) When the desk officer determines an officer's response to the scene is appropriate, the officer will forward the information to dispatch as soon as practical.
 - (e) Desk officers may be assigned other duties based on their capabilities.
- (b) If a caller is unwilling to provide the report details over the phone, or respond to the office, the desk officer should refer the incident to the shift supervisor.
- (c) When a desk officer takes a report that requires an on-scene action, such as collection of evidence, photographs, or follow-up, the desk officer will notify the on-duty supervisor as soon as practical, of the need for a patrol officer.
- (d) The desk officer will complete supplemental reports to any original report as required.
- (e) All reports shall be completed by the end of the shift, prior to going off duty. If an exception is needed, the desk officer must get approval from the shift supervisor.

1024.9 PROBATIONARY EMPLOYEES

Probationary employees who are assigned to a temporary modified-duty assignment may have their probation extended by a period of time equal to their assignment to temporary modified duty.

1024.10 MAINTENANCE OF CERTIFICATION AND TRAINING

Employees assigned to temporary modified duty shall maintain all certification, training and qualifications appropriate to both their regular and temporary duties, provided that the certification, training or qualifications are not in conflict with any medical limitations or restrictions. Employees who are assigned to temporary modified duty shall inform their supervisors of any inability to maintain any certification, training or qualifications.

Training and Professional Standards Unit

1025.1 PURPOSE AND SCOPE

- (a) The South Salt Lake Police Department maintains a training unit
 1. The unit is overseen and directed by the administrative lieutenant, who is assigned by the Chief of Police.
- (b) The training unit shall make necessary arrangements for training.
 1. Authorized training will be based upon the needs of the department, recommendations or requests from division commanders and/or sergeants, or as directed by the Office of the Chief of Police.
 2. The Chief of Police or his/her designee shall make the final decision on any training that involves a financial expenditure.

1025.1.1 POLICE OFFICER TRAINING ACADEMY

- (a) The South Salt Lake Police Department utilizes an academy certified by the State of Utah, Peace Officer's Standards and Training (POST). Utah State Law UCA 53-6-103, 104,105, establishes the legal authority for departmental participation in a POST academy.
 1. The training unit shall maintain a liaison with personnel at the Utah Division of POST.
 2. The police department may provide staff, instructors, and other resources to the academy, when approved by the Chief of Police or his/her designee.
- (b) Minimum basic training curriculum shall be established by POST and be based on job-task analysis of the most frequent assignments of officers who complete recruit training.
 1. Evaluation techniques shall be designed and utilized to measure competency in the required skills, knowledge, and abilities of a police officer.
 2. If the department feels curriculum should be introduced or changed, the training unit shall prepare a letter of request, with documentation to be signed by the Chief of Police or his/her designee.
 3. Departmental influence upon training curriculum is governed by the field officer training manual.
- (c) Department personnel may identify deficiencies in academy training, especially when the subject matter concerns topics directly related to the police department. The training coordinator shall schedule supplemental training to offset those deficiencies in the following areas:
 1. Department policies and procedures.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Training and Professional Standards Unit

2. Local criminal justice system.
 3. Certifications on various instruments used in the course of duty.
 4. Any other areas not sufficiently covered which the Supervisor/Commander feels should be addressed.
- (d) The financial relationship between the South Salt Lake City Police Department and Utah POST is governed by Utah Rules of Administrative Procedure.

1025.2 ATTENDANCE REQUIREMENTS

- (a) All personnel are required to attend assigned training.
1. The Training Unit, via the chain of command, will notify officers when they have been selected to attend outside training.
 2. Students will not leave the class while it is in session.
 3. Unexcused absences by an employee will be documented and forwarded to the officer's respective division commander.
 4. When a mandatory training class is missed, the employee will contact the training coordinator to see if makeup training can be scheduled.
 5. Makeup training is scheduled at the mutual convenience of the training unit and the employee's regular work unit.
 6. If the employee does not have an acceptable reason for missing the class, provisions for a make-up shall not be considered a high priority for the training unit, unless otherwise directed.
- (b) The following are requirements for all employees attending in-service or external training.
1. Employees attending any training are expected to fully participate and to conduct themselves in such a manner as to promote an atmosphere of learning.
 2. Students attending in-service training or training outside the department will be dressed in business casual wear, further defined as slacks or "Docker" type pants, collared shirt or polo shirt.
 - (a) Jeans may be worn if they are free of holes and clean.
 - (b) No thongs or similar footwear will be worn.
 - (c) For training involving physical activities such as ACT or firearms, the student will be notified prior to the class of the type of attire to be worn.
 3. Cell phones will be turned off or on set to "silent" and will not be answered during class. Messages can be checked and returned during the breaks.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Training and Professional Standards Unit

- (a) Sergeants and the on-call detective may keep their cell phone on while attending class, for the purpose of handling emergencies.
- 4. There will be no magazines, newspapers or other non class related materials allowed in the class room.
- 5. As with any on-duty activity, Sergeants are responsible for the behavior and compliance of officers.
- (c) When the training room is used for inter-office training or meetings, it is the responsibility of the instructor or the person reserving the room to prepare the room for its intended use. It will also be that person's responsibility to return the room to its original condition at the end of the class/ meeting.
- (d) If an employee fails to attend a class or pass required training and it results in a penalty to the employee's pay, in relation to the department pay plan, subsequent successful completion of the training will not result in retroactive payment of the penalty.
- (e) When an employee has completed a session or series of mandatory training classes, the training coordinator will document the attendance, to include the nature of the instruction and the date(s) attended.

1025.3 TRAINING LESSON PLANS AND TESTING

- (a) All training courses or programs require lesson plans. Lesson plans should include the following:
 - 1. Statement of goals or purpose.
 - 2. Performance and job-related objectives.
 - 3. Subject material to be covered.
- (b) Lesson plans will be routed to the training coordinator for approval prior to commencement of any scheduling or training.
 - 1. A copy of each approved lesson plan will be maintained in the training coordinator's files.
- (c) Training programs involving certification will also require an evaluation of each employee's learning retention, once the training has been completed.
 - 1. Such evaluation should be accomplished by a competency-based test.
 - 2. Employees are required to pass all tests given during training. Tests may include, but are not limited to:
 - (a) Written tests.
 - (b) Verbal tests.
 - (c) Minimum-scoring tests.
 - (d) Physical activity tests.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Training and Professional Standards Unit

- (e) Other tests as required.

1025.4 TYPES OF TRAINING

(a) Field Training:

1. The department Field Training Unit shall be responsible for ensuring the probationary police officers receive training in city and department policies, procedures, regulations, and rules.
2. Such training shall include issuance of all required department manuals and directives, firearms training and training in defensive tactics, arrest control and search and seizure.
3. All recruits, upon completion of the POST academy, shall be required to attend and pass a department FTO program with acceptable evaluations.
4. Failure to successfully complete the FTO program could result in an extended FTO program and/or dismissal.
5. Final decisions concerning a recruits employment will be decided by the Chief of Police in consultation with those parties involved in the recruit officers training and supervision.
6. Cause for termination during a probationary period is not required.

(b) In-Service Training:

1. The department supports the concept of in-service training.
 - (a) 40-hours of in-service training per year will be considered the minimum for all sworn employees.
 - (b) Additional training, based on the needs and benefits to the department and employee, will be an objective of the division or a departmental yearly goal, if so determined by the appropriate division commander.
 - (c) It is, however, not the legal responsibility of the department to provide training to an officer for the purpose of maintaining peace officer certification.
 - (d) In-service training will be designed to keep personnel up-to-date on new laws, technological improvements, and revisions in department standards (policy, procedure, and regulations).
 - (e) In-service training may also be designed to provide supervisory, management or specialized training to participants, and/or items of general interest and concern.
 - (f) The training coordinator will be responsible for the implementation of an in-service training program designed to keep employees proficient in their current assignments.
 - (g) In-service training may be accomplished by utilizing training officers within the department, classes offered through Utah POST, and other sources as available.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Training and Professional Standards Unit

2. In-Service Training for Career Specialty Positions:
 - (a) Additional in-service training in "specialty positions" such as hostage negotiations, special responses, and police service dogs shall also be presented not only to enhance the employee's skill level, but also to stimulate personnel to compete in new areas of interest and specialization.
 3. In-Service Training for Management Specialty Positions:
 - (a) In-service training for management personnel will be provided through mid-management workshops and appropriate classes through POST and other sources as available.
 - (b) The Chief of Police encourages and participates in informal training in management information systems, fiscal management, organizational behavior, budget preparation, and decision-making.
 4. Resources Provided to Develop in-Service Training Opportunities:
 - (a) The training coordinator will make available to all officers, a current listing of schools available through POST.
 - (b) This list will be updated at least annually.
 - (c) A list of available schools will be posted on the bulletin board in the roll-call and mail rooms.
 - (d) Any school or workshop notification received by the training coordinator, in addition to those noted above, will be posted.
 5. Refresher Training:
 - (a) Refresher training will be provided as a part of in-service training to update information on advancements in investigative processes.
 6. All sworn officers will, at least annually, prove proficiency in the use of their duty and off-duty firearms, emergency vehicle operation (EVO), OC-based pepper spray deployment, Taser, basic arrest control techniques, first aid/CPR, and may be required to pass a physical agility course at the discretion of the Chief of Police.
 7. The Chief of Police or his/her designee may exempt certain ranks or positions from training qualifications.
- (c) Employee Training:
- (a) Sworn and non-sworn employees whose responsibilities include victim/witness assistance will receive training in victim/witness rights and needs through the academy and their FTO program.
- (d) Shift Briefing Training:
- (a) Roll call training is a viable method of reinforcing past training as well as introducing new information to personnel.
 - (b) Roll call training may be impromptu or assigned by the training coordinator and/or affected supervisor.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Training and Professional Standards Unit

- (c) Roll call training may take into account the special needs of personnel who, by virtue of their assignments, are not able to participate in normally scheduled training.
- (d) The shift supervisor will coordinate planning for roll call training.
 - (a) Requests for specific training should be directed through one's immediate supervisor to the training section.
- (e) Techniques/methods used to conduct roll call training may vary depending on the nature of the material presented.
 - (a) Oral presentation may be supplemented with videotape, handouts, hands-on application, audio cassette recording, or whatever method best serves to communicate the training information.
 - (b) The South Salt Lake Police Department recognizes Utah POST as the principle source of formal training and education of its officers.
 - (a) Roll call training instruction should emphasize consistency and concurrence with POST instruction.
- (f) The training section will function as liaison with POST to ensure that mutually recognized standards of instruction are maintained.
- (g) Those personnel who participate in roll call training may provide a verbal and/or written evaluation of the training material as may be required by the training section.
- (h) The training section may coordinate the assignment and scheduling of roll call training.
- (i) Additionally, supervisors may accomplish this function by delegating the task of such training to shift officers.
- (j) Roll call training will occur as special needs arise or upon request by department personnel for this type of instruction.
- (k) Roll call training will be pre-announced in order for supervisors to schedule personnel to achieve the maximum level of attendance possible.
- (e) Specialized In-Service Training:
 - (a) Certain positions or specialized assignments within the department will require skills training prior to or shortly after appointment or promotion to the position.
 - (b) This training may be on the job, in the form of specialized schools, or it may come through department in-service training efforts.
 - (c) When practical, this training shall be initiated within thirty (30) days of appointment or promotion.
 - (d) The Chief of Police and/ or division commanders will identify the specialized assignments.
 - (e) The respective division commander will maintain a list of specialized assignments within their division.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Training and Professional Standards Unit

- (f) Specialized assignments may include but are not limited to:
 - (a) Police Service Dog Officer (PSD).
 - (b) Special Weapons and Tactics team (SWAT).
 - (c) Special Investigations.
 - (d) Internal Affairs.
 - (e) Motorcycle Officer.
 - (f) DARE / GREAT Officer.
 - (g) School Resource Officer.
 - (h) Investigator.
 - (i) Metro Gang Investigator.
 - (j) DEA Investigator.
 - (k) FBI Violent Crimes Task Force Investigator.
 - (l) Cyber Crimes Task Force Investigator.
 - (m) Hostage Negotiator.
 - (n) Crime Scene Investigator.
 - (o) Bicycle Patrol Officer.
- (g) It is the intent of the department to maximize its potential by providing specialized training that meets the needs of the individual(s) and the organization.
- (h) The training coordinator, in conjunction with supervisors and commanders, shall ensure that employees receive the appropriate training necessary to safely and completely accomplish their assignment(s).
- (i) The training coordinator will communicate directly with those supervisors overseeing officers in specialized assignments for the purpose of determining special training needs.
- (j) In many of the specialized assignments, such as the tasks forces and crime scene, the training is provided through outside sources, in some cases the training is also financed by the federal agency overseeing the task force.
- (f) Tactical Team Training:
 - 1. The South Salt Lake City Police Department participates in a part-time SWAT team.
 - 2. In order to maintain the highest degree of readiness, regular training will be held.
 - 3. This training will maintain the appropriate level of performance needed for high-risk incidents.
 - 4. An assigned sergeant will be in charge of the SWAT team..
 - 5. The team will train a minimum of 10 hours per month.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Training and Professional Standards Unit

- 6.
7. SWAT team training will consist of:
 - (a) Physical conditioning.
 - (b) Tactics and procedures necessary for deployment.
 - (c) Firearms training.
8. The SWAT team Sergeant, in conjunction with the Training Coordinator, will maintain all SWAT team training records.
- (g) Non-Sworn Employee Training:
 - (a) All employees at the police department, whether sworn or non-sworn, will be afforded training designed to promote job safety and job task understanding.
 - (b) The training may take the form of orientation training, on-the-job training, in-service training, formal schooling or any combination thereof.
 - (c) All newly hired non-sworn employees shall receive job orientation training from his/her immediate supervisor or his/her designee. Orientation training shall include, but is not limited to:
 - (a) The department's role, purpose, goals, policies, and procedures.
 - (b) The rules, regulations, and working conditions of the department as embodied in the code of conduct manual and elsewhere.
 - (c) The responsibilities of associated with a job description and the rights of the employee assigned that job classification.
 - (d) Safety matters such as the location of fire exits, first aid equipment, etc.
- (h) Instructor Training:
 1. Instructors in agency-operated training programs must have attended POST instructor development. Every instructor should know how to:
 - (a) Develop a lesson plan.
 - (b) Develop performance objective.
 - (c) Know various Instructional techniques.
 - (d) Use testing and evaluation techniques.
 - (e) Identify resource availability and use.
 2. The South Salt Lake City Police Department employs no full-time instructors.
- (i) Training Upon Promotion:
 - (a) Prior to promotion or as soon afterward as classes are available, personnel promoted to new positions will be provided with training to enable them to fulfill their new duties and responsibilities.
- (j) Remedial Training:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Training and Professional Standards Unit

- (a) Identifying an employee's job performance and comparing it the standards set for the job is the best way to determine the need for remedial training.
- (b) An employee whose job performance is determined to be lower than standard due to a lack of requisite knowledge shall become a candidate for remedial training.
- (c) Prior to recommending remedial training or performing direct action to remedy an employee's training issues, the employee's supervisor shall make a reasonable effort to determine the extent of the performance inadequacy. This may be done by:
 - (a) Reviewing the employee's performance appraisal(s).
 - (b) Direct observation of the employee's performance.
 - (c) Consultation with other department staff.
 - (d) Examination of complaint investigation reports and inspection reports pertinent to the employee's job performance.
 - (e) Examination of test scores given in training areas pertinent to the inadequate performance.
 - (f) When it has been determined that an employee's performance inadequacy should be properly dealt with via remedial training, the employee's supervisor shall provide the necessary training to correct the deficiency as soon as possible.
 - (g) Employees who fail to attend or participate in scheduled remedial training may be subject to disciplinary action up to and including termination.

1025.5 TRAINING RECORDS

- (a) The training unit will be responsible for the maintenance of all department training records.
 - 1. The training records system will be used as an integral part of the career development program and for any other authorized purposes as may benefit the employee, the department, and its goals or programs.
 - 2. Training records will be maintained and filed by employee name and other such methods as may be appropriate to the needs of the department and required through POST and state law.
 - 3. It is the responsibility of the employee who has completed training to supply the training coordinator with the written signed documentation stating that such training was received. There are three approved methods of providing the training unit with documentation of training received:
 - (a) Complete and submit a signed "Training Notification Form" along with an attached copy of any certificate received. (This method is used primarily for non-in-service training).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Training and Professional Standards Unit

- (b) Sign an inter-departmental training roster (this method is used primarily for in-service type training).
 - (c) Provide the training coordinator with training certificate.
- (b) Training files on each employee will be updated regularly to include information on new or recently received training documentation and should include at a minimum:
 - (a) The date and type of training received.
 - (b) A statement verifying attendance and the number of hours of training received.
 - (c) The results (scores) of any tests taken during the training.
 - (d) Copy of any certificate/degree awarded.
 - (e) Copy of the syllabus.
- (c) All training records are documented in your ACADIS POST portal for you to review at any time.
- (d)
- (e) Inspection of the training records system shall be conducted on an as-needed basis by the Chief of Police or his/her designee and/or the training unit.
- (f) Inter-departmental training files are used to record the type and amount of training afforded by the department. Records found in department training files should consist of, at a minimum:
 - (a) The lesson plan for the course of instruction.
 - (b) A roster of the names of each employee attending the training, along with the date of the training and the number of hours.
 - (c) If competency tests were administered, the score or pass/fail documentation of each person taking the test(s).
- (g) The training unit will keep written records pertaining to all proficiency and career specialty in-service training.

1025.6 TRAINING, SCHOOL OR FUNCTION REIMBURSEMENT PROCESS

A. When an employee is selected to attend a department approved school, training, or function, the following expenses are reimbursable:

- (a) Transportation costs:
 - (a) Airfare to/from the school/training/function.
 - (b) Use of a department vehicle and operating expenses.
 - (c) Payment of mileage at the current city rate when use of a privately owned vehicle is authorized.
- (b) City authorized per diem.
- (c) City authorized lodging expenses.
- (d) City authorized tuition and/or fees.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Training and Professional Standards Unit

- (a) Any fees for college credit, out-of-state tuition, or books, requires review and approval through the reimbursement process.
- (e) Depending on the circumstances, additional expenses may be authorized by the Chief of Police or his/her designee.
- (f) The City Training/Travel forms shall be completed with authorized signatures prior to training/travel.
- (g) If you do not attend, or leave early from approved school/training/function, for any reason, you be responsible to reimburse all cost associated.

Speech, Expression, and Social Networking

1026.1 PURPOSE AND SCOPE

This policy is intended to address issues associated with the use of social networking sites, and provides guidelines for the regulation and balancing of member speech and expression with the needs of the South Salt Lake Police Department.

This policy applies to all forms of communication including but not limited to digital media, print media, public or private speech, and use of all internet services, including the web, email, file transfer, remote computer access, news services, social networking, social media, instant messaging, blogs, forums, and other file-sharing sites.

Nothing in this policy is intended to prohibit or infringe upon any communication, speech, or expression that is protected under law. This includes speech and expression protected under state or federal constitutions as well as labor or other applicable laws. For example, this policy does not limit a member from speaking as a private citizen about matters of public concern, such as misconduct or corruption.

Members are encouraged to consult with their supervisors regarding any questions arising from the application or potential application of this policy.

1026.2 POLICY

Members of public entities occupy a trusted position in the community, and thus, their statements have the potential to contravene the policies and performance of the South Salt Lake Police Department. Due to the nature of the work and influence associated with the law enforcement profession, it is necessary that members of this [department/office] be subject to certain reasonable limitations on their speech and expression. To achieve its mission and efficiently provide service to the public, the [Department/Office] will carefully balance the individual member's rights against the needs and interests of the [Department/Office] when exercising a reasonable degree of control over its members' speech and expression.

1026.3 SAFETY

For safety and security reasons, SSLPD personnel are cautioned not to disclose their employment with the SSLPD, nor shall they post information pertaining to any other member of the department without their permission. Employees should consider carefully the implications of their speech or any other form of expression when using the Internet. Speech and expression that may negatively affect the safety of the South Salt Lake Police Department employees, such as posting personal information in a public forum, can result in compromising an employee's home address or family ties. Employees should therefore not disseminate or post any information on any forum or medium that could reasonably be anticipated to compromise the safety of any employee, an employee's family or associates. Examples of the type of information that could reasonably be expected to compromise safety include:

- Disclosing a photograph and name or address of an officer who is working undercover.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Speech, Expression, and Social Networking

- Disclosing the address of a fellow officer.
- Otherwise disclosing where another officer can be located off-duty.

As such, SSLPD personnel are cautioned not to do the following:

- a. Display SSLPD logos, uniforms, or similar identifying items on personal web pages, social media sites, or forum.
- b. SSLPD personnel are free to express themselves as private citizens on social media sites to the degree their speech does not impair working relationships of the SSLPD for which loyalty and confidentiality are important, impede the performances of duties, impair the discipline and harmony among coworkers, or negatively affect the public perception of the department.
- c. As public employees, SSLPD personnel are cautioned that speech, on or off-duty, made pursuant to their official duties is not protected speech under the First Amendment, and may be the basis for discipline, up to including termination, if deemed detrimental to the department.
- d. SSLPD employees should be aware that privacy settings and social media sites are constantly changing, and they should never assume that their personal information posted on any social media site is protected.

1026.4 DEPARTMENT SANCTIONED SOCIAL MEDIA USE

The South Salt Lake City Police Department social media sites, or pages, shall be approved by the Chief of Police, or designee, and shall be administered by the Public Information Officer or designee.

- a. Where possible, social media pages shall clearly indicate they are maintained by SSLPD and shall have all SLLPD contact information prominently displayed.
- b. Where possible, social media pages should state that the opinions expressed by visitors to the page(s) do not necessarily reflect the opinions of the SSLPD.

1026.5 PERSONAL SOCIAL MEDIA USE

Employees of the South Salt Lake City Police Department are reminded that their conduct both on and off duty must meet a high standard. This is not limited to conduct related to materials posted on the internet or disseminated electronically. Employees should note that anytime they engage in social media, they are representing the SSLPD and therefore should not do anything that will discredit themselves or SSLPD.

- a. Social media applications will not be downloaded or installed on department issued equipment unless authorized by the Chief of Police and in accordance with South Salt lake City IT Policy.
- b. As such, no employee will allow or permit any information to be posted to the internet that:
 1. Could reasonably be interpreted to express the opinions of the SSLPD. An employee may comment on a subject of general interest and of value and concern to the public provided that, in doing so, the employee does not suggest or imply that the views expressed are those of SSLPD.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Speech, Expression, and Social Networking

2. Has both a reference to the employee being affiliated with SSLPD and which contains content that is unprofessional, unbecoming, or illegal, such as:

- a. Speech containing obscene or sexually explicit language, profanity, images, or acts;
- b. Statements or other forms of speech that ridicule, malign, disparage, or otherwise express bias against any race, any religion, or any protected class of individuals;
- c. Excessive alcohol consumption;
- d. Speech, or images involving themselves or other SSLPD personnel which displays behavior that would reasonably be considered reckless or irresponsible. Employees are reminded that courts may scrutinize the credibility of a witness from unintentional sources like the internet.
- e. Could reasonably be interpreted as having an adverse effect upon agency morale, discipline, operation of the agency, safety of staff or perception of the public.
- f. Contains any recording, including images, obtained while engaged in the performance of enforcement activities, tactical situations, or any department assignment that may have an adverse effect upon the agency. Posting digital images of certain activities such as police sponsored community events, promotions, etc. may be permissible. Clarification on appropriate postings, if needed, will be directed to the Chief of Police, public information officer or designee.

1026.6 PROHIBITED SPEECH, EXPRESSION, AND CONDUCT

To meet the safety, performance, and public-trust needs of the South Salt Lake Police Department, the following are prohibited unless the speech is otherwise protected (e.g., a member speaking as a private citizen on a matter of public concern):

- (a) Speech or expression made pursuant to an official duty that tends to compromise or damage the mission, function, reputation, or professionalism of the [Department/Office] or its members.
- (b) Speech or expression that, while not made pursuant to an official duty, is significantly linked to, or related to, the [Department/Office] and tends to compromise or damage the mission, function, reputation, or professionalism of the [Department/Office] or its members. Examples may include:
 - 1. Statements that indicate disregard for the law or the state or U.S. Constitutions.
 - 2. Expression that demonstrates support for criminal activity.
 - 3. Participation in sexually explicit photographs or videos for compensation or distribution.
- (c) Speech or expression that could reasonably be foreseen as having a negative impact on the credibility of the member as a witness. For example, posting to a website statements or expressions that glorify or endorse dishonesty, unlawful discrimination, or illegal behavior.
- (d) Speech or expression of any form that could reasonably be foreseen as having a negative impact on the safety of the members of the [Department/Office] (e.g., a statement on a blog that provides specific details as to how and when prisoner

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Speech, Expression, and Social Networking

transportations are made could reasonably be foreseen as potentially jeopardizing members by informing criminals of details that could facilitate an escape or attempted escape).

- (e) Speech or expression that is contrary to the canons of the Law Enforcement Code of Ethics as adopted by the [Department/Office].
- (f) Use or disclosure, through whatever means, of any information, photograph, digital media, or other recording obtained or accessible as a result of employment or appointment with the [Department/Office] for financial or personal gain, or any disclosure of such materials without the express authorization of the Chief of Police or the authorized designee (Utah Code 67-16-4).
- (g) Posting, transmitting, or disseminating any photographs, digital media or audio recordings, likenesses or images of [department/office] logos, emblems, uniforms, badges, patches, marked vehicles, equipment, or other material that specifically identifies the South Salt Lake Police Department on any personal or social networking or other website or web page, without the express authorization of the Chief of Police.

Members must take reasonable and prompt action to remove any content, including content posted by others, that is in violation of this policy from any web page or website maintained by the member (e.g., social or personal website).

1026.6.1 UNAUTHORIZED ENDORSEMENTS AND ADVERTISEMENTS

While members are not restricted from engaging in the following activities as private citizens, members may not represent the South Salt Lake Police Department or identify themselves in any way that could be reasonably perceived as representing the [Department/Office] in order to do any of the following, unless specifically authorized by the Chief of Police (Utah Code 20A-11-1206):

- (a) Endorse, support, oppose, or contradict any political campaign or initiative.
- (b) Endorse, support, oppose, or contradict any social issue, cause, or religion.
- (c) Endorse, support, or oppose any product, service, company, or other commercial entity.
- (d) Appear in any commercial, social, or nonprofit publication; or any motion picture, film, video, or public broadcast; or on any website.
- (e) Use the email of South Salt Lake Police Department for any political purpose (Utah Code 20A-11-1205).

Additionally, when it can reasonably be construed that a member, acting in their individual capacity, is affiliated with this [department/office], the member shall give a specific disclaiming statement that any such speech or expression is not representative of the South Salt Lake Police Department.

Members retain their rights to vote as they choose, to support candidates of their choice, and to express their opinions as private citizens on political subjects and candidates at all times while off-duty. However, members may not use their official authority or influence to interfere with or affect the result of elections or nominations for office. Members are also prohibited from directly

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Speech, Expression, and Social Networking

or indirectly using their official authority to coerce, command, or advise another member to pay, lend, or contribute anything of value to a party, committee, organization, agency, or person for political purposes (5 USC § 1502).

1026.7 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to emails, texts, or anything published or maintained through file-sharing software or any internet site, including social media, that is accessed, transmitted, received, or reviewed on any [department/office] technology system (see the Information Technology Use Policy for additional guidance).

The [Department/Office] may not require a member to disclose a username and/or password that allows access to the member's personal internet accounts (Utah Code 34-48-201).

1026.8 CONSIDERATIONS

In determining whether to grant authorization of any speech or conduct that is prohibited under this policy, the factors that the Chief of Police or the authorized designee should consider include:

- (a) Whether the speech or conduct would negatively affect the efficiency of delivering public services.
- (b) Whether the speech or conduct would be contrary to the good order of the [Department/Office] or the efficiency or morale of its members.
- (c) Whether the speech or conduct would reflect unfavorably upon the [Department/Office].
- (d) Whether the speech or conduct would negatively affect the member's appearance of impartiality in the performance of their duties.
- (e) Whether similar speech or conduct has been previously authorized.
- (f) Whether the speech or conduct may be protected and outweighs any interest of the [Department/Office].

1026.9 TRAINING

Subject to available resources, the [Department/Office] should provide training regarding the limitations on speech, expression, and use of social networking to all members of the [Department/Office].

POLICE OFFICER II - PROMOTIONAL CAREER ENHANCEMENT

1027.1 PURPOSE AND POLICY

It shall be the policy of this police department to encourage and assist officers in achieving advancement within their chosen discipline and to provide departmental standards to enhance an officer's progress within the promotional career enhancement program.

1027.1.1 DEFINITIONS

Probationary Officer: an officer with less than one year of service with the South Salt Lake Police Department.

Probationary Period: a probationary officer remains on probation until one year following the completion of the assigned field training program.

POI: Is a pay grade status

POII: Is a promotional pay grade status.

POII Probationary Period: Once promoted to a POII, the officer will be on probationary status for one year.

1027.1.2 PROCEDURES

- A. An officer who believes they qualify for the Police Officer II-Promotional Career Enhancement, must submit an application to the Office of the Chief of Police or designee at any point once eligible. Each application shall include supporting documentation for verification for eligibility.

1027.1.3 QUALIFICATIONS

- A. Applicant must:
 - 1. Be employed as a Police Officer I with the South Salt Lake City Police Department.
 - 2. Completed four (4) years of continuous service with the South Salt Lake Police Department.
 - 3. Have attended and completed Crisis Intervention Team (CIT) certification (40 hours) and currently CIT Certified.
 - 4. Have obtained POST Mid-Management Certificate.
 - 5. Complete a minimum of three years in a full-time specialty service, or three years in two part-time specialty assignments or credit for the education conversion. Any combination of specialty service and/or education that equals three years may be submitted for review.
- B.
 - 1. Complete a minimum of three years in a full-time specialty with the South Salt Lake Police Department. Full-time specialty are defined as:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

POLICE OFFICER II - PROMOTIONAL CAREER ENHANCEMENT

- (a) School Resource/Youth Resource Officer
- (b) Homeless Resource Officer
- (c) Community Resource Officer
- (d) K-9 Officer
- (e) Traffic/Motors Officer
- (f) Detective

C.1. Complete a minimum of three years in two part-time specialty assignment. The two part-time specialty assignments may run simultaneously. Part-time assignments are defined as:

- (a) Bike Patrol
- (b) S.W.A.T.
- (c) Honor Guard
- (d) Public Order Unit
- (e) Field Training Officer
- (f) Major Accident Team
- (g) Mobil Incident Command Center (M.I.C.C.)
- (h) Designated Department Training Instructor
- (i) Alternate Motors
- (j) UAS Operator
- (k) Public Information Officer and Alternate Public Information Officer
- (l) Peer Support

D..Police Officers will receive the following credit for:

- Associates Degree or 60 Credit Hours = 1 year of specialty assignment.
- Bachelors Degree = 2 years of specialty assignments.
- Masters Degree = 3 years of specialty assignments combination of a full-time specialty assignment, part-specialty assigned and/or formal education must equal the minimum three year requirements.

E. The application is the promotional process to obtain the POII designation

F. All applications are subject to approval by the Chief of Police or designee.

G. If application is approved and applicant is promoted to POII, there may be additional duties assigned to assist in supervisory functions. Applicant will not be assigned to cover a full shift, but may be tasked with covering a squad for no more that two hours, on a limited, approved basis. POII is not an OIC or Corporal designee,

Anti-Retaliation

1028.1 PURPOSE AND SCOPE

This policy prohibits retaliation against members who identify workplace issues, such as fraud, waste, abuse of authority, gross mismanagement, or any inappropriate conduct or practices, including violations that may pose a threat to the health, safety, or well-being of members (Utah Code 53-6-210.5).

This policy does not prohibit actions taken for nondiscriminatory or non-retaliatory reasons, such as discipline for cause (Utah Code 53-6-210.5).

These guidelines are intended to supplement and not limit members' access to other applicable remedies. Nothing in this policy shall diminish the rights or remedies of a member pursuant to any applicable federal law, provision of the U.S. Constitution, law, ordinance, or collective bargaining agreement.

1028.2 POLICY

The South Salt Lake Police Department has a zero tolerance for retaliation and is committed to taking reasonable steps to protect from retaliation members who, in good faith, engage in permitted behavior or who report or participate in the reporting or investigation of workplace issues. All complaints of retaliation will be taken seriously and will be promptly and appropriately investigated.

1028.3 RETALIATION PROHIBITED

No member may retaliate against any person for engaging in lawful or otherwise permitted behavior; for opposing a practice believed to be unlawful, unethical, discriminatory or retaliatory; for reporting or making a complaint under this policy; or for participating in any investigation related to a complaint under this or any other policy.

Retaliation includes any adverse action or conduct, including but not limited to:

- Refusing to hire or denying a promotion.
- Extending the probationary period.
- Unjustified reassignment of duties or change of work schedule.
- Real or implied threats or other forms of intimidation to dissuade the reporting of wrongdoing or filing of a complaint, or as a consequence of having reported or participated in protected activity.
- Taking unwarranted disciplinary action.
- Spreading rumors about the person filing the complaint or about the alleged wrongdoing.
- Shunning or unreasonably avoiding a person because he/she has engaged in protected activity.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Anti-Retaliation

1028.4 COMPLAINTS OF RETALIATION

Any member who feels he/she has been retaliated against in violation of this policy should promptly report the matter to any supervisor, command staff member, Chief of Police or the City Director of Human Services.

Members shall act in good faith, not engage in unwarranted reporting of trivial or minor deviations or transgressions, and make reasonable efforts to verify facts before making any complaint in order to avoid baseless allegations. Members shall not report or state an intention to report information or an allegation knowing it to be false, with willful or reckless disregard for the truth or falsity of the information or otherwise act in bad faith.

Investigations are generally more effective when the identity of the reporting member is known, thereby allowing investigators to obtain additional information from the reporting member. However, complaints may be made anonymously. All reasonable efforts shall be made to protect the reporting member's identity. However, confidential information may be disclosed to the extent required by law or to the degree necessary to conduct an adequate investigation and make a determination regarding a complaint. In some situations, the investigative process may not be complete unless the source of the information and a statement by the member is part of the investigative process.

1028.5 SUPERVISOR RESPONSIBILITIES

Supervisors are expected to remain familiar with this policy and ensure that members under their command are aware of its provisions.

The responsibilities of supervisors include but are not limited to:

- (a) Ensuring complaints of retaliation are investigated as provided in the Personnel Complaints Policy.
- (b) Receiving all complaints in a fair and impartial manner.
- (c) Documenting the complaint and any steps taken to resolve the problem.
- (d) Acknowledging receipt of the complaint, notifying the Chief of Police via the chain of command and explaining to the member how the complaint will be handled.
- (e) Taking appropriate and reasonable steps to mitigate any further violations of this policy.
- (f) Monitoring the work environment to ensure that any member making a complaint is not subjected to further retaliation.
- (g) Periodic follow-up with the complainant to ensure that retaliation is not continuing.
- (h) Not interfering with or denying the right of a member to make any complaint.
- (i) Taking reasonable steps to accommodate requests for assignment or schedule changes made by a member who may be the target of retaliation if it would likely mitigate the potential for further violations of this policy.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Anti-Retaliation

1028.6 COMMAND STAFF RESPONSIBILITIES

The Chief of Police should communicate to all supervisors the prohibition against retaliation.

Command staff shall treat all complaints as serious matters and shall ensure that prompt actions take place, including but not limited to:

- (a) Communicating to all members the prohibition against retaliation.
- (b) The timely review of complaint investigations.
- (c) Remediation of any inappropriate conduct or condition and instituting measures to eliminate or minimize the likelihood of recurrence.
- (d) The timely communication of the outcome to the complainant.

1028.7 WHISTLE-BLOWING

The Utah Protection of Public Employees Act protects an employee who (Utah Code 67-21-1 et seq.):

- (a) Communicates in good faith the waste or misuse of public funds, property, or manpower.
- (b) Communicates in good faith a suspected violation of a state or federal law, rule, or regulation.
- (c) Objects to or refuses to carry out a directive that the member reasonably believes violates state or federal law.

Members who believe they have been the subject of retaliation for engaging in such protected behaviors should promptly report it to a supervisor. Supervisors should refer the complaint to the Professional Standards Unit for investigation pursuant to the Personnel Complaints Policy.

1028.7.1 NOTICE OF EMPLOYEE PROTECTIONS AND OBLIGATIONS

The Department shall post a notice and use appropriate means to keep employees informed of their protections and obligations under the Utah Protection of Public Employees Act. The Department shall provide the employee with a copy of the Act (Utah Code 67-21-9):

- (a) When the employee is hired.
- (b) Upon a request by the employee.
- (c) When the employee files a grievance under the Utah Protection of Public Employees Act.

1028.8 RECORDS RETENTION AND RELEASE

The Records Supervisor shall ensure that documentation of investigations is maintained in accordance with the established records retention schedules.

1028.9 TRAINING

The policy should be reviewed with each new member.

All members should receive periodic refresher training on the requirements of this policy.

Workplace Violence

1029.1 PURPOSE AND SCOPE

The South Salt Lake Police Department institutes this policy as part of its commitment to a safer and more supportive organizational climate and to the prevention and reduction of the incidence and effects of domestic violence, sexual violence, and stalking [hereinafter "violence"] at the workplace. The department recognizes that domestic violence, sexual violence, and stalking present unique issues for its workforce.

Domestic violence, sexual violence, and stalking are workplace issues even if incidents occur elsewhere. Domestic violence, sexual violence, and stalking cross economic, educational, cultural, age, gender, racial, and religious lines and occur in a wide variety of contexts. Therefore, the department will take every appropriate measure to prevent and/or address such violence in the context of:

- Subordinate/superior relationships;
- Heterosexual and same-sex intimate partner relationships, including marital, cohabiting, or dating;
- Heterosexual or same sex non-intimate partner relationships, such as between coworkers;
- Parent/child relationships; and
- Violent acts of others that could potentially occur within the workplace.

The purposes and goals of this policy are to:

1. Support a comprehensive workplace education and training program to prevent violence and promote healthy relationships for employees and their families;
2. Create a supportive and healthful work environment that helps employees to avoid the use of violence in any context;
3. Institutionalize responsive policies and procedures to assist employees who are impacted by violence, including the provision of training on this policy to employees and management;
4. Provide assistance to employees who are perpetrators of violence and take disciplinary action to hold them accountable for violent behavior; and
5. Provide immediate assistance and support to survivors of violence, such as information and referrals to community resources, to facilitate safety and support for survivors and fellow employees.

1029.2 STATEMENT OF CONFIDENTIALITY

South Salt Lake Police Department recognizes and respects an employee's right to privacy and the need for confidentiality and autonomy.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Workplace Violence

South Salt Lake Police Department shall maintain the confidentiality of an employee's disclosure regarding violence to the extent allowed by law, and unless to do so would result in physical harm to any person, and/or jeopardize safety within the workplace. When information must be disclosed to protect the safety of individuals within the workplace.

South Salt Lake Police Department shall limit the breadth and content of such disclosure to information reasonably necessary to protect the safety of the disclosing employee and others, and to comply with the law.

South Salt Lake Police Department shall provide advance notice to the employee who disclosed information, to the extent possible, if the disclosure must be shared with other parties in order to maintain safety in the workplace or elsewhere.

South Salt Lake Police Department shall also provide the employee with the name and title of the person to whom the South Salt Lake Police Department intends to share the employee's statements, and shall explain the necessity and purpose regarding said disclosure.

1029.3 PERSONS COVERED BY THIS POLICY

Persons covered by this policy include: Any South Salt Lake Police Department employee to include full and part-time employees, interns, contractors, volunteers, or temporary workers.

Wellness Program

1030.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance on establishing and maintaining a proactive wellness program for [department/office] members.

The wellness program is intended to be a holistic approach to a member's well-being and encompasses aspects such as physical fitness, mental health, and overall wellness.

Additional information on member wellness is provided in the:

- Line-of-Duty Deaths Policy.
- Drug- and Alcohol-Free Workplace Policy.

1030.1.1 DEFINITIONS

Definitions related to this policy include:

Critical incident – An event or situation that may cause a strong emotional, cognitive, or physical reaction that has the potential to interfere with daily life.

Critical Incident Stress Debriefing (CISD) – A standardized approach using a discussion format to provide education, support, and emotional release opportunities for members involved in work-related critical incidents.

Peer support – Mental and emotional wellness support provided by peers trained to help members cope with critical incidents and certain personal or professional problems.

Peer support member – A member of the South Salt Lake Police Department who has been trained in peer support skills and has been appointed to the [department/office] peer support team (Utah Code 78B-5-902).

Peer support specialist – An individual in sustained recovery from substance use or mental health disorders who has obtained the proper training certificate and passed the required exam through the Utah Department of Health and Human Services (Utah Code 26B-5-102; UAC R523-5-8).

1030.2 POLICY

It is the policy of the South Salt Lake Police Department to prioritize member wellness to foster fitness for duty and support a healthy quality of life for [department/office] members. The [Department/Office] will maintain a wellness program that supports its members with proactive wellness resources, critical incident response, and follow-up support.

1030.3 WELLNESS COORDINATOR

The Chief of Police should appoint a trained wellness coordinator. The coordinator should report directly to the Chief of Police or the authorized designee and should collaborate with advisers (e.g., Department of Human Resources, legal counsel, licensed psychotherapist, qualified health

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Wellness Program

professionals), as appropriate, to fulfill the responsibilities of the position, including but not limited to:

- (a) Identifying wellness support providers (e.g., licensed psychotherapists, external peer support providers, physical therapists, dietitians, physical fitness trainers holding accredited certifications).
 - 1. As appropriate, selected providers should be trained and experienced in providing mental wellness support and counseling to public safety personnel.
 - 2. When practicable, the [Department/Office] should not use the same licensed psychotherapist for both member wellness support and fitness for duty evaluations.
- (b) Developing management and operational procedures for [department/office] peer support members, such as (Utah Code 78B-5-903):
 - 1. Peer support member selection and retention.
 - 2. Training and applicable certification requirements.
 - 3. Deployment.
 - 4. Managing potential conflicts between peer support members and those seeking service.
 - 5. Monitoring and mitigating peer support member emotional fatigue (i.e., compassion fatigue) associated with providing peer support.
 - 6. Using qualified peer support personnel from other public safety agencies or outside organizations for [department/office] peer support, as appropriate.
- (c) Verifying members have reasonable access to peer support or licensed psychotherapist support.
- (d) Establishing procedures for CISDs, including:
 - 1. Defining the types of incidents that may initiate debriefings.
 - 2. Steps for organizing debriefings.
- (e) Facilitating the delivery of wellness information, training, and support through various methods appropriate for the situation (e.g., phone hotlines, electronic applications).
 - 1. Information on mental health resources shall be provided to members annually, including how to access mental health resources and directions on how to appeal a denial of mental health resources as required by Utah Code 53-21-102.
- (f) Verifying a confidential, appropriate, and timely Employee Assistance Program (EAP) is available for members. This also includes:
 - 1. Obtaining a written description of the program services.
 - 2. Providing for the methods to obtain program services.
 - 3. Providing referrals to the EAP for appropriate diagnosis, treatment, and follow-up resources.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Wellness Program

4. Obtaining written procedures and guidelines for referrals to, or mandatory participation in, the program.
 5. Obtaining training for supervisors in their role and responsibilities, and identification of member behaviors that would indicate the existence of member concerns, problems, or issues that could impact member job performance.
- (g) Assisting members who have become disabled with application for federal government benefits such as those offered through the Public Safety Officers' Benefits Program (34 USC § 10281 et seq.).
1. The coordinator should work with appropriate [Department/Office] liaisons to assist qualified members and survivors with benefits, wellness support, and counseling services, as applicable, when there has been a member death (see the Line-of-Duty Deaths Policy for additional guidance).
- (h) Serving as the designated mental health resources liaison and providing the Department of Public Safety with their current contact information (Utah Code 53-21-102).

1030.4 CRITICAL INCIDENT STRESS DEBRIEFINGS

A Critical Incident Stress Debriefing should occur as soon as practicable following a critical incident. The coordinator is responsible for organizing the debriefing. Notes and recorded statements shall not be taken because the sole purpose of the debriefing is to help mitigate the stress-related effects of a critical incident.

The debriefing is not part of any investigative process. Care should be taken not to release or repeat any communication made during a debriefing unless otherwise authorized by policy, law, or a valid court order.

Attendance at the debriefing should only include peer support members and those directly involved in the incident.

1030.5 PEER SUPPORT COMMUNICATIONS

The [Department/Office] will honor the sensitivity of confidential communications with peer support members, communication which are not confidential are outlined per Utah State Code 78B-5-903.

1030.5.1 RESTRICTIONS ON DISCLOSURE OF PEER SUPPORT COMMUNICATIONS

A peer support team member acting in that capacity and according to South Salt Lake Police Department guidelines for provision of peer support services may not be compelled to testify or disclose records regarding peer support sessions in court proceedings unless specific exceptions apply (Utah Code 78B-5-903).

1030.6 PHYSICAL WELLNESS PROGRAM

The coordinator is responsible for establishing guidelines for any on-duty physical wellness program, including the following:

- (a) Voluntary participation by members

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Wellness Program

- (b) Allowable physical fitness activities
- (c) Permitted times and locations for physical fitness activities
- (d) Acceptable use of [department/office]-provided physical fitness facilities and equipment.
- (e) Individual health screening and fitness assessment
- (f) Individual education (e.g., nutrition, sleep habits, proper exercise, injury prevention) and goal-setting
- (g) Standards for fitness incentive programs. The coordinator should collaborate with the appropriate entities (e.g., human resources, legal counsel) to verify that any standards are nondiscriminatory.
- (h) Maintenance of physical wellness logs (e.g., attendance, goals, standards, progress)
- (i) Ongoing support and evaluation

1030.7 MENTAL HEALTH SUPPORT

The [Department/Office] shall provide or make available mental health resources, as defined by Utah Code 53-21-101, to qualified members, their spouses and children (including certain surviving spouses), and certain retired and separated members and their spouses, as required by law (Utah Code 53-21-102).

Any access of mental health resources provided by the [Department/Office] shall be kept confidential.

1030.8 WELLNESS PROGRAM AUDIT

At least annually, the coordinator or the authorized designee should audit the effectiveness of the [department/office]'s wellness program and prepare a report summarizing the findings. The report shall not contain the names of members participating in the wellness program, and should include the following information:

- Data on the types of support services provided
- Wait times for support services
- Participant feedback, if available
- Program improvement recommendations
- Policy revision recommendations

The coordinator should present the completed audit to the Chief of Police for review and consideration of updates to improve program effectiveness.

1030.9 TRAINING

The coordinator or the authorized designee should collaborate with the Training Coordinator to provide all members with regular education and training on topics related to member wellness, including but not limited to:

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Wellness Program

- The availability and range of [department/office] wellness support systems.
- Suicide prevention.
- Recognizing and managing mental distress, emotional fatigue, post-traumatic stress, and other possible reactions to trauma.
- Alcohol and substance disorder awareness.
- Countering sleep deprivation and physical fatigue.
- Anger management.
- Marriage and family wellness.
- Benefits of exercise and proper nutrition.
- Effective time and personal financial management skills.

Training materials, curriculum, and attendance records should be forwarded to the Training Coordinator as appropriate for inclusion in training records.

Line-of-Duty Deaths

1031.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance to members of the South Salt Lake Police Department in the event of the death of a member occurring in the line of duty and to direct the [Department/Office] in providing proper support for the member's survivors.

The Chief of Police may also apply some or all of this policy for a non-line-of-duty member death, or in situations where members are injured in the line of duty and the injuries are life-threatening.

1031.1.1 DEFINITIONS

Definitions related to this policy include:

Line-of-duty death - The death of an officer during the course of performing law enforcement-related functions while on- or off-duty, or a non-sworn member during the course of performing assigned duties.

For an officer, a line-of-duty death includes death that is the direct and proximate result of a personal injury sustained in the line of duty (34 USC § 10281).

Survivors - Immediate family members of the deceased member, which can include spouse, children, parents, other next of kin, or significant others. The determination of who should be considered a survivor for purposes of this policy should be made on a case-by-case basis given the individual's relationship with the member and whether the individual was previously designated by the deceased member.

1031.2 POLICY

It is the policy of the South Salt Lake Police Department to make appropriate notifications and to provide assistance and support to survivors and coworkers of a member who dies in the line of duty.

It is also the policy of this department to respect the requests of the survivors when they conflict with these guidelines, as appropriate.

1031.3 INITIAL ACTIONS BY COMMAND STAFF

- (a) Upon learning of a line-of-duty death, the deceased member's supervisor should provide all reasonably available information to the Watch Commander and Dispatch.
 - 1. Communication of information concerning the member and the incident should be restricted to secure networks to avoid interception by the media or others (see the Public Information Officer section of this policy).
- (b) The Watch Commander should ensure that notifications are made in accordance with the Officer-Involved Shootings and Deaths and Major Incident Notification policies as applicable.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Line-of-Duty Deaths

- (c) If the member has been transported to the hospital, the Watch Commander or the authorized designee should respond to the hospital to assume temporary responsibilities as the Hospital Liaison.
- (d) The Chief of Police or the authorized designee should assign members to handle survivor notifications and assign members to the roles of Hospital Liaison (to relieve the temporary Hospital Liaison) and the [Department/Office] Liaison as soon as practicable (see the Notifying Survivors section and the [Department/Office] Liaison and Hospital Liaison subsections in this policy).

1031.4 NOTIFYING SURVIVORS

Survivors should be notified as soon as possible in order to avoid the survivors hearing about the incident in other ways.

The Chief of Police or the authorized designee should review the deceased member's emergency contact information and make accommodations to respect the member's wishes and instructions specific to notifying survivors. However, notification should not be excessively delayed because of attempts to assemble a notification team in accordance with the member's wishes.

The Chief of Police, Watch Commander, or the authorized designee should select at least two members to conduct notification of survivors, one of which may be the [Department/Office] chaplain.

Notifying members should:

- (a) Make notifications in a direct and compassionate manner, communicating as many facts of the incident as possible, including the current location of the member. Information that is not verified should not be provided until an investigation has been completed.
- (b) Determine the method of notifying surviving children by consulting with other survivors and taking into account factors such as the child's age, maturity, and current location (e.g., small children at home, children in school).
- (c) Plan for concerns such as known health concerns of survivors or language barriers.
- (d) Offer to transport survivors to the hospital, if appropriate. Survivors should be transported in [department/office] vehicles. Notifying members shall inform the Hospital Liaison over a secure network that the survivors are on their way to the hospital. Notifying members should remain at the hospital while the survivors are present.
- (e) When survivors are not at their residences or known places of employment, actively seek information and follow leads from neighbors, other law enforcement, postal authorities, and other sources of information in order to accomplish notification in as timely a fashion as possible. Notifying members shall not disclose the reason for their contact other than a family emergency.
- (f) If making notification at a survivor's workplace, ask a workplace supervisor for the use of a quiet, private room to meet with the survivor. Members shall not inform the

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Line-of-Duty Deaths

workplace supervisor of the purpose of their visit other than to indicate that it is a family emergency.

- (g) Offer to call other survivors, friends, or clergy to support the survivors and to avoid leaving survivors alone after notification.
- (h) Assist the survivors with meeting child care or other immediate needs.
- (i) Provide other assistance to survivors and take reasonable measures to accommodate their needs, wishes, and desires. Care should be taken not to make promises or commitments to survivors that cannot be met.
- (j) Inform the survivors of the name and phone number of the Survivor Support Liaison (see the Survivor Support Liaison section of this policy), if known, and the [Department/Office] Liaison.
- (k) Provide their contact information to the survivors before departing.
- (l) Document the survivors' names and contact information, as well as the time and location of notification. This information should be forwarded to the [Department/Office] Liaison.
- (m) Inform the Chief of Police or the authorized designee once survivor notifications have been made so that other South Salt Lake Police Department members may be apprised that survivor notifications are complete.

1031.4.1 OUT-OF-AREA NOTIFICATIONS

The Department Liaison should request assistance from law enforcement agencies in appropriate jurisdictions for in-person notification to survivors who are out of the area.

- (a) The Department Liaison should contact the appropriate jurisdiction using a secure network and provide the assisting agency with the name and telephone number of the department member that the survivors can call for more information following the notification by the assisting agency.
- (b) The Department Liaison may assist in making transportation arrangements for the member's survivors, but will not obligate the Department to pay travel expenses without the authorization of the Chief of Police.

1031.5 NOTIFYING [DEPARTMENT/OFFICE] MEMBERS

Supervisors or members designated by the Chief of Police are responsible for notifying [department/office] members of the line-of-duty death as soon as possible after the survivor notification is made. Notifications and related information should be communicated in person or using secure networks and should not be transmitted over the radio.

Notifications should be made in person and as promptly as possible to all members on-duty at the time of the incident. Members reporting for subsequent shifts within a short amount of time should be notified in person at the beginning of their shifts. Members reporting for duty from their residences should be instructed to contact their supervisors as soon as practicable. Those members who are working later shifts or are on days off should be notified by phone as soon as practicable.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Line-of-Duty Deaths

Members having a close bond with the deceased member should be notified of the incident in person. Supervisors should consider assistance (e.g., peer support, modifying work schedules, approving sick leave) for members who are especially affected by the incident.

Supervisors should direct members not to disclose any information outside the [Department/Office] regarding the deceased member or the incident.

1031.6 LIAISONS AND COORDINATORS

The Chief of Police or the authorized designee should select members to serve as liaisons and coordinators to handle responsibilities related to a line-of-duty death, including but not limited to:

- (a) [Department/Office] Liaison.
- (b) Hospital Liaison.
- (c) Survivor Support Liaison.
- (d) Wellness Support Liaison.
- (e) Funeral Liaison.
- (f) Mutual aid coordinator.
- (g) Benefits Liaison.
- (h) Finance coordinator.

Liaisons and coordinators will be directed by the [Department/Office] Liaison and should be given sufficient duty time to complete their assignments.

Members may be assigned responsibilities of more than one liaison or coordinator position depending on available [department/office] resources. The [Department/Office] Liaison may assign separate liaisons and coordinators to accommodate multiple family units, if needed. The [Department/Office] should consider seeking assistance from surrounding law enforcement agencies to fill liaison and coordinator positions, as appropriate.

1031.6.1 DEPARTMENT/OFFICE LIAISON

The [Department/Office] Liaison should be a Division Commander or of sufficient rank to effectively coordinate [department/office] resources, and should serve as a facilitator between the deceased member's survivors and the [Department/Office]. The [Department/Office] Liaison reports directly to the Chief of Police. The [Department/Office] Liaison's responsibilities include but are not limited to:

- (a) Directing the other liaisons and coordinators in fulfilling survivors' needs and requests. Consideration should be given to organizing the effort using the National Incident Management System.
- (b) Establishing contact with survivors within 24 hours of the incident and providing them contact information.
- (c) Advising survivors of the other liaison and coordinator positions and their roles and responsibilities.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Line-of-Duty Deaths

- (d) Identifying locations that will accommodate a law enforcement funeral and presenting the options to the appropriate survivors, who will select the location.
- (e) Coordinating all official law enforcement notifications and arrangements.
- (f) Making necessary contacts for authorization to display flags at half-staff.
- (g) Reminding [department/office] members of appropriate information-sharing restrictions regarding the release of information that could undermine future legal proceedings.
- (h) Coordinating security checks of the member's residence as necessary and reasonable.
- (i) Serving as a liaison with visiting law enforcement agencies during memorial and funeral services.

1031.6.2 HOSPITAL LIAISON

The Hospital Liaison should work with hospital personnel to:

- (a) Establish a command post or incident command system, as appropriate, to facilitate management of the situation and its impact on hospital operations (e.g., influx of people, parking).
- (b) Arrange for appropriate and separate waiting areas for:
 - 1. The survivors and others whose presence is requested by the survivors.
 - 2. [Department/Office] members and friends of the deceased member.
 - 3. Media personnel.
- (c) Ensure, as practicable, that any suspects who are in the hospital and their families or friends are not in proximity to the member's survivors or South Salt Lake Police Department members (except for members who may be guarding a suspect).
- (d) Arrange for survivors to receive timely updates regarding the member before information is released to others.
- (e) Arrange for survivors to have private time with the member, if requested.
 - 1. The Hospital Liaison or hospital personnel may need to explain the condition of the member to the survivors to prepare them accordingly.
 - 2. The Hospital Liaison should accompany the survivors into the room, if requested.
- (f) Stay with survivors and provide them with other assistance as needed at the hospital.
- (g) If applicable, explain to the survivors why an autopsy may be needed.
- (h) Make arrangements for hospital bills to be directed to the [Department/Office], that the survivors are not asked to sign as guarantor of payment for any hospital treatment, and that the member's residence address, insurance information, and next of kin are not included on hospital paperwork.

Other responsibilities of the Hospital Liaison include but are not limited to:

- Arranging transportation for the survivors back to their residence.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Line-of-Duty Deaths

- Working with investigators to gather and preserve the deceased member's equipment and other items that may be of evidentiary value.
- Documenting their actions at the conclusion of duties.

1031.6.3 SURVIVOR SUPPORT LIAISON

The Survivor Support Liaison should work with the [Department/Office] Liaison to fulfill the immediate needs and requests of the survivors of any member who has died in the line of duty, and serve as the long-term [department/office] contact for survivors.

The Survivor Support Liaison should be selected by the deceased member's Division Commander. The following should be considered when selecting the Survivor Support Liaison:

- The liaison should be an individual the survivors know and with whom they are comfortable working.
- The selection may be made from names recommended by the deceased member's supervisor and/or coworkers. The deceased member's partner or close friends may not be the best selections for this assignment because the emotional connection to the member or survivors may impair their ability to conduct adequate liaison duties.
- The liaison must be willing to assume the assignment with an understanding of the emotional and time demands involved.

The responsibilities of the Survivor Support Liaison include but are not limited to:

- (a) Arranging for transportation of survivors to hospitals, places of worship, funeral homes, and other locations, as appropriate.
- (b) Communicating with the [Department/Office] Liaison regarding appropriate security measures for the family residence, as needed.
- (c) If requested by the survivors, providing assistance with instituting methods of screening telephone calls made to their residence after the incident.
- (d) Providing assistance with travel and lodging arrangements for out-of-town survivors.
- (e) Returning the deceased member's personal effects from the [Department/Office] and the hospital to the survivors. The following should be considered when returning the personal effects:
 1. Items should not be delivered to the survivors until they are ready to receive the items.
 2. Items not retained as evidence should be delivered in a clean, unmarked box.
 3. All clothing not retained as evidence should be cleaned and made presentable (e.g., items should be free of blood or other signs of the incident).
 4. The return of some personal effects may be delayed due to ongoing investigations.
- (f) Assisting with the return of [department/office]-issued equipment that may be at the deceased member's residence.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Line-of-Duty Deaths

1. Unless there are safety concerns, the return of the equipment should take place after the funeral at a time and in a manner considerate of the survivors' wishes.
- (g) Working with the Wellness Support Liaison for survivors to have access to available counseling services.
- (h) Coordinating with the [department/office]'s Public Information Officer (PIO) to brief the survivors on pending press releases related to the incident and to assist the survivors with media relations in accordance with their wishes (see the Public Information Officer section of this policy).
- (i) Briefing survivors on investigative processes related to the line-of-duty death, such as criminal, internal, and administrative investigations.
- (j) Informing survivors of any related criminal proceedings and accompanying them to such proceedings.
- (k) Introducing survivors to prosecutors, victim's assistance personnel, and other involved personnel as appropriate.
- (l) Maintaining long-term contact with survivors and taking measures to sustain a supportive relationship (e.g., follow-up visits, phone calls, cards on special occasions, special support during holidays).
- (m) Inviting survivors to [department/office] activities, memorial services (e.g., as applicable, the Annual Candlelight Vigil at the National Law Enforcement Officers Memorial), or other functions as appropriate.

Survivor Support Liaisons providing services after an incident resulting in multiple members being killed should coordinate with and support each other through conference calls or meetings as necessary.

The [Department/Office] recognizes that the duties of a Survivor Support Liaison will often affect regular assignments over many years, and is committed to supporting members in the assignment.

If needed, the Survivor Support Liaison should be issued a personal communication device (PCD) owned by the [Department/Office] to facilitate communications necessary to the assignment. The [department/office]-issued PCD shall be used in accordance with the Personal Communication Devices Policy.

1031.6.4 WELLNESS SUPPORT LIAISON

The Wellness Support Liaison should work with the [department/office] wellness coordinator or the authorized designee and other liaisons and coordinators to make wellness support and counseling services available to members and survivors who are impacted by a line-of-duty death. The responsibilities of the Wellness Support Liaison include but are not limited to:

- (a) Identifying members who are likely to be significantly affected by the incident and may have an increased need for wellness support and counseling services, including:
 1. Members involved in the incident.
 2. Members who witnessed the incident.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Line-of-Duty Deaths

3. Members who worked closely with the deceased member but were not involved in the incident.
- (b) Making arrangements for members who were involved in or witnessed the incident to be relieved of [department/office] responsibilities until they can receive wellness support.
- (c) Making wellness support and counseling resources (e.g., peer support, Critical Incident Stress Debriefing) available to members as soon as reasonably practicable following the line-of-duty death.
- (d) Coordinating with the Survivor Support Liaison to inform survivors of available wellness support and counseling services and assisting with arrangements as needed.
- (e) Following up with members and the Survivor Support Liaison in the months following the incident to determine if additional wellness support or counseling services are needed.

1031.6.5 FUNERAL LIAISON

The Funeral Liaison should work with the [Department/Office] Liaison, Survivor Support Liaison, and survivors to coordinate funeral arrangements to the extent the survivors wish. The Funeral Liaison's responsibilities include but are not limited to:

- (a) Assisting survivors in working with the funeral director regarding funeral arrangements and briefing them on law enforcement funeral procedures.
- (b) Completing funeral notification to other law enforcement agencies.
- (c) Coordinating the funeral activities of the [Department/Office], including but not limited to the following:
 1. Honor Guard
 - (a) Casket watch
 - (b) Color guard
 - (c) Pallbearers
 - (d) Bell/rifle salute
 2. Bagpipers/bugler
 3. Uniform for burial
 4. Flag presentation
 5. Last radio call
- (d) Briefing the Chief of Police and command staff concerning funeral arrangements.
- (e) Assigning an officer to remain at the family home during the viewing and funeral.
- (f) Arranging for transportation of the survivors to and from the funeral home and interment site using [department/office] vehicles and drivers.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Line-of-Duty Deaths

- (g) Addressing event-related logistical matters (e.g., parking, visitor overflow, public assembly areas).

1031.6.6 MUTUAL AID COORDINATOR

The mutual aid coordinator should work with the [Department/Office] Liaison and the Funeral Liaison to request and coordinate any assistance from outside law enforcement agencies needed for, but not limited to:

- (a) Traffic control during the deceased member's funeral.
- (b) Area coverage so that as many South Salt Lake Police Department members can attend funeral services as possible.

The mutual aid coordinator should perform duties in accordance with the Outside Agency Assistance Policy.

Where practicable, the Chief of Police should appoint a mutual aid coordinator to identify external resources in advance of any need (e.g., regional honor guard teams, county- or state-wide resources).

1031.6.7 BENEFITS LIAISON

The Benefits Liaison should provide survivors with information concerning available benefits and will assist them in applying for benefits. Responsibilities of the Benefits Liaison include but are not limited to:

- (a) Confirming the filing of workers' compensation claims and related paperwork (see the Occupational Disease and Work-Related Injury and Death Reporting Policy).
- (b) Researching and assisting survivors with application for federal government survivor benefits, such as those offered through the following:
 - 1. Public Safety Officers' Benefits Program, including financial assistance available through the Public Safety Officers' Educational Assistance (PSOEA) Program, as applicable (34 USC § 10281 et seq.).
 - 2. Social Security Administration.
 - 3. Department of Veterans Affairs.
- (c) Researching and assisting survivors with application for state and local government survivor benefits.
 - (a) Death benefits available under Title 49, Utah State Retirement and Insurance Benefit Act
 - (b) Health coverage benefits (Utah Code 53-17-201)
 - (c) Death benefit assistance (Utah Code 53-17-501)
 - (d) Educational benefits (Utah Code 53H-11-306)
- (d) Researching and assisting survivors with application for other survivor benefits such as:
 - 1. Private foundation survivor benefits programs.

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Line-of-Duty Deaths

2. Survivor scholarship programs.
- (e) Researching and informing survivors of support programs sponsored by police associations and other organizations.
- (f) Documenting and informing survivors of inquiries and interest regarding public donations to the survivors.
 1. If requested, working with the finance coordinator to assist survivors with establishing a process for the receipt of public donations.
- (g) Providing survivors with a summary of the nature and amount of benefits applied for, including the name of a contact person at each benefit office. Printed copies of the summary and benefit application documentation should be provided to affected survivors.
- (h) Maintaining contact with the survivors and assisting with subsequent benefit questions and processes as needed.

1031.6.8 FINANCE COORDINATOR

The finance coordinator should work with the Chief of Police and the Department Liaison to manage financial matters related to the line-of-duty death. The finance coordinator's responsibilities include, but are not limited to:

- (a) Establishing methods for purchasing and monitoring costs related to the incident.
- (b) Providing information on finance-related issues, such as:
 1. Paying survivors' travel costs if authorized.
 2. Transportation costs for the deceased.
 3. Funeral and memorial costs.
 4. Related funding or accounting questions and issues.
- (c) Working with the Benefits Liaison to establish a process for the receipt of public donations to the deceased member's survivors.
- (d) Providing accounting and cost information as needed.

1031.7 PUBLIC INFORMATION OFFICER

In the event of a line-of-duty death, the [department/office]'s PIO should be the [department/office]'s contact point for the media. As such, the PIO should coordinate with the [Department/Office] Liaison to:

- (a) Collect and maintain the most current incident information and determine what information should be released.
- (b) Instruct [department/office] members to direct any media inquiries to the PIO.
- (c) Prepare necessary press releases.
 1. Coordinate with other entities having media roles (e.g., outside agencies involved in the investigation or incident).

South Salt Lake Police Department

South Salt Lake PD Policy Manual

Line-of-Duty Deaths

2. Disseminate important public information, such as information on how the public can show support for the [department/office] and deceased member's survivors.
- (d) Arrange for community and media briefings by the Chief of Police or the authorized designee as appropriate.
- (e) Respond, or coordinate the response, to media inquiries.
- (f) If requested, assist the member's survivors with media inquiries.
1. Brief the survivors on handling sensitive issues such as the types of questions that reasonably could jeopardize future legal proceedings.
- (g) Release information regarding memorial services and funeral arrangements to [department/office] members, other agencies, and the media as appropriate.
- (h) If desired by the survivors, arrange for the recording of memorial and funeral services via photos and/or video.

The identity of deceased members should be withheld until the member's survivors have been notified. If the media have obtained identifying information for the deceased member prior to survivor notification, the PIO should request that the media withhold the information from release until proper notification can be made to survivors. The PIO should notify media when survivor notifications have been made.

1031.8 INVESTIGATION OF THE INCIDENT

The Chief of Police should make necessary assignments to conduct thorough investigations of any line-of-duty death and may choose to use the investigation process outlined in the Officer-Involved Shootings and Deaths Policy.

Investigators from other agencies may be assigned to work on any criminal investigation related to line-of-duty deaths. Partners, close friends, or personnel who worked closely with the deceased member should not have any investigative responsibilities because such relationships may impair the objectivity required for an impartial investigation of the incident.

Involved [department/office] members should be kept informed of the progress of the investigations and provide investigators with any information that may be pertinent to the investigations.

1031.9 LINE-OF-DUTY DEATH OF A LAW ENFORCEMENT ANIMAL

The Chief of Police may authorize appropriate memorial and funeral services for law enforcement animals killed in the line of duty.

1031.10 NON-LINE-OF-DUTY DEATH

The Chief of Police may authorize certain support services for the death of a member not occurring in the line of duty.

South Salt Lake PD Policy Manual

South Salt Lake PD Policy Manual

Attachments

**POII Career Enhancement August
2023 Application Form.pdf**

**South Salt Lake Police Department
Career Enhancement Program
Police Officer II**

Purpose

To provide departmental standards to enhance officers progress within the career enhancement program.

Policy

It shall be the department policy to encourage and assist officers to achieve advancement within their chosen discipline. To that end, a career enhancement program establishing the requirements to become a Police Officer II.

Definitions

Recruit Officer:	A probationary officer with less than one year of service with the South Salt Lake Police Department.
P.O. I:	A police officer who has successfully completed their one year probation period.
P.O. II:	A police officer who has completed four (4) years or more of continuous employment with the South Salt Lake Police Department and meets the specified requirements for Police Officer II.

Procedures

Submission

An officer who believes they may qualify for Police Officer II may submit their application at any point throughout the year. Each application shall be as complete as

SOUTH SALT LAKE POLICE DEPARTMENT CAREER ENHANCEMENT POLICE OFFICER II APPLICATION

Date Submitted: _____

Applicants Name: _____

Employment/HIRE Date: _____

Qualifications:

	Documented	Verified
1. Police Officer I with South Salt Lake Police Department.	_____	_____
2. Completed four (4) years with the South Salt Lake Police Department.	_____	_____
3. Have attended and completed Crisis Intervention Team (CIT) training. Attach certification and current CIT Officer Status.	_____	_____
4. Certification in at least three (3) of the following: (Include documentation)		
• Instructor Development	_____	_____
• Field Training Officer	_____	_____
• Interview & Interrogation	_____	_____
• Advanced Officer	_____	_____
• Advanced Accident Investigation	_____	_____
• Street Survival Course	_____	_____
• Supervisor Course	_____	_____
• Chief Approved Advanced Training	_____	_____
5. Specialty Units: Served the minimum 3 years:	Dates Served	Verified
• Detectives/Metro Gangs	_____ to _____	_____
• Traffic/Motors	_____ to _____	_____
• K-9	_____ to _____	_____
• Street Crimes Unit	_____ to _____	_____
• Crime Resource Unit	_____ to _____	_____
• Homeless Resource Unit	_____ to _____	_____
6. Specialty Assignments: Served the minimum 3 years:	Dates Served	Verified
• Bike Patrol	_____ to _____	_____
• S.W.A.T.	_____ to _____	_____
• Honor Guard	_____ to _____	_____
• Public Order Unit	_____ to _____	_____
• Field Training Officer	_____ to _____	_____
• Major Accident Team/Alternate Motors	_____ to _____	_____
• Mobil Incident Command Center (M.I.C.C.)	_____ to _____	_____
• UAS Operator	_____ to _____	_____
• Alternate Public Information Officer	_____ to _____	_____
• Designated Department Training Instructor	_____ to _____	_____
• Peer Support	_____ to _____	_____

7. **Education: (Documentation must be included)**

Documented Verified

- Associates Degree or 60 Credit Hours
- Bachelors Degree
- Masters Degree

_____	_____
_____	_____
_____	_____

Applicant Officers Signature

Date

Police Officer II Career Enhancement

Chief of Police Review/Approval: _____

Date: _____

Applicant Notified By: _____

Date: _____

Private Persons Temporary Detention Form .pdf

PRIVATE PERSON'S TEMPORARY DETENTION FORM

(For Use by Non-Law Enforcement Individuals)

1. DETAINEE INFORMATION

- **Full Name:** _____
- **Gender:** _____
- **Date of Birth (if known):** _____
- **Address (if known):** _____
- **Phone Number (if known):** _____
- **Description (if unknown):**
Height: _____ Weight: _____ Hair Color: _____ Eye Color: _____
Clothing Description: _____

2. INCIDENT DETAILS

- **Date of Detention:** _____
- **Time of Detention:** From _____ AM/PM to _____ AM/PM
- **Location of Detention:** _____
- **Reason for Detention (Check all that apply):**
 - ☐ Suspected Theft
 - ☐ Trespassing
 - ☐ Vandalism
 - ☐ Assault
 - ☐ Other (describe): _____
- **Description of Incident (include what was observed, actions taken, etc.):**

3. DETAINING PERSON INFORMATION

- **Full Name:** _____
- **Phone Number:** _____
- **Address:** _____
- **Email:** _____
- **Relationship to Property/Location (if any):**
 - ☐ Owner
 - ☐ Employee

SOUTH SALT LAKE POLICE TEMPORARY DETENTION FORM

- ☐ Bystander/Witness
 - ☐ Security (Private)
 - ☐ Other: _____
-

4. ACTION TAKEN

- Was law enforcement contacted? ☐ Yes ☐ No
 - Agency contacted: _____
 - Time contacted: _____ AM/PM
 - Name/Badge # of officer (if available): _____
 - Was force used? ☐ Yes ☐ No
- If yes, describe the nature of force used and why:
- _____
- _____
-

5. WITNESS(ES) (if any)

- Name: _____
 - Contact Info: _____
 - Statement (optional): _____
-
-

6. SIGNATURES

I, the undersigned, affirm that the above information is true to the best of my knowledge and that I have detained the individual in accordance with applicable laws until law enforcement could respond.

Signature of Detaining Person: _____ Date: _____

Signature of Witness (if applicable): _____ Date: _____

**axon_onepager_taserengeryweaponcomparison_17x11_04a-
digital.pdf**

AXON'S TASER ENERGY WEAPONS COMPARISON



/ TASER 10
10 cartridges featuring individually targeted probes.



/ TASER 7
Two cartridge types for Close Quarters and Stand-off situations, with dual laser including range adjusting lower laser.



/ TASER X26P
Single cartridge legacy weapon.



/ TASER X2
Two cartridge legacy weapon.

RELEASE DATE	2023	2018	2013	2011
RANGE ¹	45 feet (13.72 meters)	25 feet (7.62 meters)	25 feet (7.62 meters)	25 feet (7.62 meters)
CARTRIDGE CAPACITY	10	2	1	2
INDIVIDUALLY TARGETED PROBES	Yes	No	No	No
CROSS-CONNECT CAPABILITY	Any Probe Connect ²	Adaptive Cross-Connect	N/A	Cross-Connect
ILLUMINATION	210 lumen LED flashlight (1000 lumen strobing in warning mode)	210 lumen LED flashlight	—	—
LASER(S)	Class 3R Green LASER or Class 2 Red available	Top - Class 3R or Class 2 Green LASER Bottom - Class 3R or Class 2 Red LASER	Red Class 3R Class 2 LASER available	Red Class 3R Class 2 LASER available
STEALTH MODE	Yes	Yes	No	No
DE-ESCALATION	Warning Alert	Warning Arc	N/A	Warning Arc
VR INTEGRATION	Yes	Yes	No	No
AUTOMATED ARMORY	Yes	Yes	No	No
DOCK AND WALK WORKFLOW	Yes	Yes	No	No
RECHARGEABLE BATTERY PACK	Yes	Yes	No	No
CID DISPLAY	Yes	Yes	Yes	Yes
WEATHER RESISTANT	Dust and water ingress protection to International Ingress Protection IP67	Dust and water ingress protection to International Ingress Protection IP53	Dust and water ingress protection to International Ingress Protection IP52	Dust and water ingress protection to International Ingress Protection IP52
OPERATING TEMPERATURE	-4 to 122 degrees F (-10 to 50 degrees C)	-4 to 122 degrees F (-10 to 50 degrees C)	-4 to 122 degrees F (-10 to 50 degrees C)	-4 to 122 degrees F (-10 to 50 degrees C)
DROP TEST	5 feet (1.5 meters)	4 feet (1.2 meters)	4 feet (1.2 meters)	4 feet (1.2 meters)
HUMIDITY	95% non-condensing	95% non-condensing	80% non-condensing	80% non-condensing
USEFUL LIFE	5 Years	5 Years	5 years	5 years
COLOR AVAILABILITY	Axon Yellow	Axon Yellow	Black & Axon Yellow	Black & Axon Yellow

¹ Actual wire length may exceed specified useable range.

² Spread Optimizer energizes up to 4 probes at once.

GSD-SSL SRO Interlocal Agreement 7.29.24 (1).pdf

SCHOOL RESOURCE OFFICER INTERLOCAL COOPERATION AGREEMENT

THIS SCHOOL RESOURCE OFFICER INTERLOCAL COOPERATION AGREEMENT (the Agreement"), is made and entered into on the 18th day of July 2024 by and between South Salt Lake City ("City"), a political subdivision of the State of Utah, and the BOARD OF EDUCATION OF GRANITE SCHOOL DISTRICT (the "School District"), a political subdivision of the State of Utah, 2500 South State Street, Salt Lake City, Utah 84115.

WITNESSETH

WHEREAS, pursuant to the provisions of the Utah Interlocal Cooperation Act, Utah Code Annotated §11-13-101, et seq., as amended, public agencies, including political subdivisions of the State of Utah as defined therein, are authorized to enter into mutually advantageous agreements for joint or cooperative action; and

WHEREAS, pursuant to the provisions of the Utah Code Annotated, §53G-8-703, which provides that the School District may contract with a law enforcement agency to provide school resource officer services at the schools pursuant to Board review and approval of this Agreement; and

WHEREAS, the School District and South Salt Lake City, through their respective governing bodies, have voluntarily determined that the interests and welfare of the public within their respective jurisdictions will best be served by this Agreement to provide for joint and cooperative action in regard to having a School Resource Officer ("SRO") to maintain safe schools, improve school climate, and support educational opportunities for students while serving at Granite Park Junior High School ("The School"); and

WHEREAS, the governing bodies of the School District and City have agreed to adopt this Agreement to provide for the joint and cooperative action contained herein; and

WHEREAS, this Agreement shall replace and supersede any agreements or memoranda of understanding approved and executed previously, if any, by the School District and City regarding an SRO.

NOW, THEREFORE, be it mutually covenanted and agreed as follows, each of the parties accepting as consideration for this Agreement the mutual promises and agreements of the other:

EFFECTIVE DATE AND DURATION

This Agreement shall be deemed effective as of August 1, 2024, and shall continue for a period of five (5) years thereafter, terminating on July 30, 2029, unless sooner terminated as provided herein. Following the initial five-year term, this agreement shall be automatically renewed for

successive one-year periods unless either party requests termination or modification of this agreement. Such a request will be made in writing.

ADMINISTRATIVE ENTITY

City and the School District do not contemplate nor intend to establish a separate legal entity under their terms of this Agreement.

PURPOSE

This Agreement is established for the purpose of jointly providing for one (1) SRO to serve at The School.

MANNER OF FINANCING

This Agreement and the matters contemplated herein shall not receive separate financing, nor shall a separate budget be required. Each party shall be responsible for its own obligations under this Agreement. City shall budget and be responsible for all payments related to the employment of the SRO. City shall send an invoice to the School District quarterly for payment of the services as agreed in writing between the School District and City, which total cost to the School District is \$45,000 per year for the initial five-year term of this Agreement. Thereafter, the parties may mutually agree on an annual cost for subsequent years of this Agreement; failing such mutual agreement, this Agreement shall be deemed terminated. The invoices shall be paid within sixty (60) days of receipt by the School District. If this Agreement is terminated during the budget year, City and the School District agree to divide the costs associated with the payment of the services of the SRO as on a pro rata basis depending on the length of the year remaining.

ADMINISTRATOR

Pursuant to Utah Code Annotated, §11-13-101, et seq., the parties agree that City shall act as administrator responsible for this Agreement. This Agreement does not anticipate nor provide for any organizational changes in City or the School District.

FILING OF AGREEMENT

A copy of this Agreement shall be placed on file in the Recorder's Office of City and with the Chief of Granite Police Department ("GPD") and shall remain on file for public inspection during the term of this Agreement.

DESCRIPTION OF ARRANGEMENT

1. City Obligations and Responsibilities:

- a. The SRO shall be an employee of City and shall be subject to the administration, supervision, and control of City.
- b. City will ensure that the SRO is a trained and certified law enforcement officer. City and School District shall work together to provide SRO-specific training required under Utah Code Annotated, §53G-8-702.
- c. City will pay the costs for the police officer to support the SRO services in excess of the amounts due from the School District. City will furnish uniforms and any equipment that state law requires for provision of the SRO services or that the parties jointly agree is necessary for the provision of the SRO services.
- d. Scheduling, deployment, and supervision of the SRO will be the responsibility of City. The hours of SRO availability will be during normal school hours while school is in session based on the District-approved calendar.
- e. In the event of an SRO taking preapproved leave in excess of three (3) days, the City is responsible for finding a substitute. The City shall not be responsible to provide a substitute SRO for an unforeseen absence due to illness or other events that do not extend beyond three (3) days.
- f. The SRO shall be subject to all personnel policies and practices of City except as such policies or practices may be modified by the terms and conditions of this Agreement.
- g. City, in its sole discretion, shall have the power and authority to hire, discharge, and discipline the SRO; however, the School District and City will jointly discuss SRO assignments.
- h. As an employee of City, the SRO will be subject to the chain of command of City.
- i. If the principal of The School is dissatisfied with an SRO who has been assigned to that principal's school, that principal may request that the City Chief of Police assign a different officer as the SRO for that school. Such a request to the City Chief of Police will occur after the principal has met with the SRO's Supervisor to discuss concerns and allow for a reasonable amount of time for the SRO's Supervisor to remediate the issues unless the concerns are of such a nature, in the opinion of the principal, to warrant an immediate replacement. The City Chief of Police shall make every reasonable effort to expeditiously assign a new SRO to that school. City reserves the right to remove/re-assign any SRO after reasonable notification has been given to the School District.

- j. The SRO and the principal, or designee, will jointly complete the SRO training describe in Utah Code Annotated §53G-8-702. Whenever possible, SRO training will occur during non-school hours or on days when school is not in session. The SRO may also be invited to attend additional training with SROs from GPD.
- k. The City Chief of Police and the School District's Superintendent (the "Superintendent"), or their designees, shall determine the working hours of the SRO supporting the SRO services, taking into account The District calendar. The hours of SRO availability will be during normal school hours while The School is in session. Adjustments outside of these regular hours shall be by mutual agreement in writing between that school's principal and City's designee.
- 1. Although the SRO remains a City employee, the SRO is required to be on campus unless performing duties directly related to the SRO services off campus. In such cases, the SRO shall attempt to inform the principal prior to the event, but if prior notice is not possible, the SRO shall report and explain the absence as soon as possible afterward to the principal.
 - i. City shall ensure that the SRO Supervisor maintains communication with the schools' administrators throughout the school year to evaluate the performance of services provided by the SRO.
 - ii. City will provide the School District with a "point of contact" to facilitate communications regarding SRO services. City's point of contact for the schools shall be the SRO Supervisor.
 - iii. The SRO shall provide immediate assistance to address the criminal conduct of persons other than students.
- n. At the request of the school, the SRO will teach a vocational law enforcement class.
- o. The City will at least annually, seek out and accept feedback from the school about SRO performance.
- p. The City will be responsible for providing SROs for school events that are outside of school hours including athletic events, school dances, etc. The School District will hire at an hourly rate of \$50 / per hour.
- q. Allegations of a criminal nature against school staff members wherein the alleged criminal behavior occurred on school property will be referred to Granite School District Police Department.
- 2. School District Obligations and Responsibilities:
 - a. School District shall communicate with the SRO Supervisor regarding removal/reassignment of an SRO.

- b. In the unlikely event that a situation arises wherein the School District believes that a particular SRO's presence at a school, facility, or event constitutes a direct and immediate threat to the safety and well-being of the School District community, the School District may direct the SRO to leave the premises and not return until the School District has resolved the issue with either the City or the SRO.
- c. The School District shall:
 - i. Provide City with a "point of contact" to facilitate SRO services communications. The School District's point of contact for the schools shall be Chief Randy Porter, Granite Police Department.
 - ii. Provide an office/storage or workspace for the SRO's materials and personal effects.
 - iii. Provide time for school principals or designees and the assigned SRO to attend SRO training.
 - iv. Coordinate response to and differentiate between disciplinary issues and criminal problems. School administrators will handle routine administrative and school discipline (code of conduct) issues within the school without involving the SRO in an enforcement capacity unless the administrator determines that SRO involvement is necessary to address a threat to the safety of students, staff and/or patrons. School administrators are solely responsible for handling routine administrative and school discipline (code of conduct) issues that do not meet the elements of a crime.
 - v. When appropriate, administration shall discuss criminal conduct with the SRO and whether the conduct requires administrative intervention.
 - vi. Arrange meetings with the SRO as needed by school administration.
 - vii. Invite SRO to school-wide trainings regarding school code of conduct and discipline, de-escalation, Positive Behavioral Interventions and Support ("PBIS"), Multitiered Systems of Supports ("MTSS") and restorative practices provided to faculty.
 - viii. Request SRO assistance immediately to address the criminal conduct of persons other than students.
 - ix. Assist with any SRO-initiated investigation as needed.
 - x. Provide ongoing feedback to the City designee for SRO evaluation purposes.
 - xi. Notify responding SRO when a student involved in an investigation or incident requiring the assistance of the SRO has a disability and/or an

Individualized Education Program ("IEP") or Section 504 Plan, and who therefore may require special treatment or accommodations.

- xii. School principals shall provide access to students when law enforcement officers or DCFS officers are investigating allegations of child abuse subject to School District policies.

3. Mutual Obligations and Responsibilities:

- a. City and School District recognize the importance of ensuring that the SRO work collaboratively with school and district administrators. Therefore, selection of the SRO will be made through a collaborative process involving the City and School District. To be assigned an SRO, a police officer shall meet the following requirements:
 - i. The SRO shall be a fully certified law enforcement officer.
 - ii. The SRO shall possess an even temperament, be trained in de-escalation techniques and procedures, and be able to set a good example for students.
 - iii. The SRO shall possess effective communications skills that will enable the officer to function effectively within the students and school staff.
- b. Notwithstanding the foregoing, City shall make the final decision as to the placement of the SRO.
- c. City and School District are jointly responsible for ensuring that the training required under Utah Code Annotated §53G-8-703(g) is provided and completed by the SRO and principal, or designee, before the beginning of each academic year. The training may include:
 - i. Childhood and adolescent development and techniques for motivating and otherwise working with youth;
 - ii. Responding age-appropriately to students;
 - iii. Working with students with disabilities;
 - iv. Techniques to de-escalate and resolve conflict;
 - v. Cultural awareness;
 - vi. Implicit bias;
 - vii. Problems of disproportionate minority impact;
 - viii. Restorative justice practices;
 - ix. Responsibilities under the Fourteenth Amendment;

- x. Identification of students exposed to violence or trauma and making referrals to appropriate resources;
 - xi. Student privacy rights;
 - xii. Negative consequences and stigmatization associated with youth involvement in the juvenile and criminal justice systems;
 - xiii. Strategies to reduce juvenile justice involvement;
 - xiv. The role and distinctions between an SRO and other school staff who help to keep a school secure;
 - xv. Developing and supporting successful relationships with students; and
 - xvi. Legal parameters of searching and questioning students on school property.
- d. If additional training becomes required by law, ordinances, court orders, or other contractual agreements, City and School District shall jointly ensure that such training is provided and occurs.
 - e. The parties' point of contact shall meet twice each school year to discuss how the SRO services are functioning and any specific needs or concerns of the schools and SRO.
 - f. Both parties agree to discuss SRO applicants together.
 -  g. Both parties agree to the designations in §53G-8-211 which identify the student offenses that the SRO can refer to juvenile court, confer with the School to resolve, or refer to School administration for resolution with an administrator, understanding that the school will keep the SRO informed on resolution of the issue.
 - h. Both parties agree that the School will not require or prohibit mandatory rotations of SROs.
4. Duties of School Resource Officer:
- a. One SRO will be assigned to The School to provide for and maintain a safe, healthy and productive learning environment, act as a positive role model to students, build partnerships, enhance community-policing activities, identify problems within the school, develop problem solving strategies with school administrators and staff, and collaboratively develop a comprehensive school safety plan with school administrators, staff, and the District's Risk Management, and work to create a cooperative, proactive, and problem-solving approach between law enforcement and the school.
 - b. The SRO shall provide presentations to the school in safety, crime prevention, and bullying.

- c. The SRO shall provide adequate notice to the SRO's Supervisor and the school principal or designee when absent from work due to illness, training, vacation, or an agency emergency for the assignment a substitute SRO or other arrangement.
- d. The SRO and City Police Chief who oversees the SRO program will meet regularly with school principals to identify problems and work toward resolution or problems occurring in the schools.
- e. SRO will work closely with the School to improve the social and behavioral skills of students to maximize their ability to achieve academically and become successful, contributing citizens. Issues to be addressed include substance abuse, violence reduction, social skills, and other areas of district and community concerns.
- f. City and the School District understand the SRO may secure school property per established Granite School District Police Department protocols in the event of an emergency that requires shelter-in-place or lock-down.
- g. SRO services will include providing outreach to school administrators, parents, students, businesses, and the community for stakeholder involvement in problem solving and solutions with the intent of promoting collaboration and relationship building that will benefit the whole community. This collective effort will help City to provide the best public safety services and protection to all citizens and while garnering support for law enforcement.
- h. The SRO shall initiate positive interactions with students in general areas of the school to promote the profession of police officers and be a positive role model.
- i. The SRO will use de-escalation techniques whenever possible in resolving conflict or other potentially volatile situations.
- j. The SRO will be responsible for enforcing the law and is not responsible for handling routine school discipline issues. Infractions of school rules shall be handled at the school level. SROs shall be available to the school for advice, assistance, and consultation. Absent a threat to an individual or public safety, student conduct that occurs on school property involving public order offenses including disorderly conduct, disturbance/disruption of schools or school activities; loitering; profanity; and fighting that does not involve physical injury or a weapon (as defined in Utah Code §76-1-601(5)), shall be considered school discipline issues to be handled by school administrators. However, if SROs become aware of policy and code violations, SROs can assist administrators by alerting administrators and/or escorting students to the office.
- k. The SRO shall confer with the principal or designated school administrator to resolve issues that constitute minor violation of criminal law, such as Class C Misdemeanors and Infractions.

1. The SRO will be involved in school discipline if it pertains to preventing a disruption that would, if ignored, place students, faculty, staff, or other individuals at risk of harm.
- m. The SRO will share information, subject to the restrictions and requirements of the Utah Bureau of Criminal Identification, with the school's administrators about persons and conditions pertaining to campus safety concerns.
- n. The SRO shall notify the parents of the student and school administration as soon as possible upon removing a student from campus.
- o. If a student arrest is warranted at school, in a school vehicle, or at a school event, the SRO shall use only that force that is reasonably necessary and the least disruptive tactics to effectuate the arrest. The SRO will be accompanied by a school principal or vice principal when arresting a student unless emergency circumstances require otherwise for the safety of the student, the SRO, and/or others.
- p. An arrest of a student may occur on school property or at school sponsored activities when:
 - i. The SRO has probable cause to believe that the student has been or is engaged in a crime that:
 1. Poses a real or immediate threat of injury;
 2. Causes property damage;
 3. Involves the possession or uses of drugs or weapons; or
 4. The arrest is necessary to execute a warrant that cannot be effectively executed outside of School hours.
- q. The SRO shall notify the parents of the student and the applicable school administrator as soon as possible when students are arrested or ticketed.
- r. The SRO shall question students in a manner and a time when it has the least impact on the student's schooling so long as the delay in questioning does not interfere with the effectiveness of an investigation.
- s. The SRO will emphasize the use of restorative approaches to address negative student behavior.
- t. An SRO may conduct investigatory stops or detentions of students on school property or at school sponsored events when the officer has reasonable suspicion to believe that the student has been, is, or is about to be engaged in the commission of a crime.
- u. In any instance in which it becomes necessary for an SRO and/or a City police officer to detain, question, or search a minor student on school property or at a

school sponsored activity, the SRO and/or the City police officer will make reasonable efforts to ensure that a school administrator is present, except in the case of emergency circumstances or investigations into allegations of child abuse.

- v. An SRO or other City police officer may conduct an immediate, warrantless search or seizure under emergency conditions if there is probable cause to believe that delay in getting a warrant would result in the loss of evidence, escape of the suspect, or harm to the police or public. However, the SRO or City officers shall not conduct a search with a school administrator present as a means of avoiding the requirement of articulating probable cause for the search.
- w. An SRO or other City police officer is allowed to enter a School District school, property, or activity when a suspect retreats into the school, property, or activity and there is reasonable fear of escape, destruction of evidence, or injury to the police or public. Entry may also be made where a person's health, welfare or safety is concerned.
- x. Interviews of students by law enforcement personnel about matters unrelated to school shall be conducted away from school during non-school hours.
- y. The SRO or City shall provide a biannual report (in January and June) to the School District that documents each of the following incidents of law enforcement activity," in compliance with the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §12329 et seq., 34 CFR Part 99, and Utah's Student Privacy and Data Protection Act (SPDPA), Utah Code §53E-9-101 et. seq.
 - i. Arrests, including the reason the student was arrested;
 - ii. Search and seizure;
 - iii. Issuance of a criminal citation;
 - iv. Issuance of a ticket or summons;
 - v. Filing a delinquency petition; or
 - vi. Referral to a probation officer.
- z. The SRO and the school principal or assistant principal shall complete the SRO training from §53G-8-702.

5. Students Rights:

- a. An SRO may conduct or participate in a search of a student's person, possessions, or locker only where there is probable cause to believe that the search will turn up evidence that the child has committed or is committing a criminal offense.
 - i. The SRO shall inform school administrators prior to conducting a probable cause search where practicable.

- ii. The SRO shall not ask school officials to conduct a search to circumvent students' rights or protections.
 - b. A school official may conduct a search of a student's person, possessions, or locker where there is a reasonable suspicion to believe that the search will turn up evidence that the student has violated or is violating either that law or the rules of the school, and the search is justified in scope given such suspicion. Absent a cognizable threat to another student, an employee, or to other individuals, a school official shall not ask an SRO to be present or participate in such a search, although an SRO may be requested to remain in the vicinity and intercede if the search produces evidence of criminal conduct.
 - c. SROs may interrogate minor students about criminal conduct that could expose the student to court-involvement or arrest subject to constitutional rights (Miranda) and the requirements and exceptions of Utah Code §78A-6-1 12.5, including requirements for parents/guardians to be present during interrogations.
 - i. The SRO shall inform school administrators prior to questioning the student where practical.
 - ii. The SRO shall not ask a school official to question a student to circumvent any constitutional protections or protections under state law.
 - d. If an exigent circumstance or immediate threat exists, a school official or SRO may question a student about criminal conduct or conduct a search of a student's person and possessions.
 - e. Unduly invasive searches (i.e., strip searches) of students by either school officials or SRO is prohibited.
 - f. An SRO shall not use physical force or restraints on a student, including handcuffs, tasers, mace, or other physical or chemical restraints unless a student's actions pose a threat to him/herself or to others.
6. Access to Education Records:
- a. All SROs are designated as "school officials" for the purposes of the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §12329 et seq., 34 CFR Part 99, and Utah's Student Privacy and Data Protection Act (SPDPA), Utah Code §53E-9-101 et seq. As such, SROs have the right to inspect and copy any public records, including directory information, maintained by the school to the extent allowed by law. Access to student records is governed by the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §12329 et seq., 34 CFR Part 99, and Utah's Student Privacy and Data Protection Act (SPDPA), Utah Code §53E-9-101 et seq.
 - b. If additional information in a student's record is needed in an emergency to protect the health or safety of the student or other individuals, school officials

shall disclose to the SRO only that information that is needed to respond to the emergency situation based on the seriousness of the threat to someone's health or safety; the need of the information to meet the emergency situation; and the extent to which time is of the essence.

- c. Notwithstanding any of the above, if an SRO or City's law enforcement officer presents a warrant, subpoena, or court order for special educational records or video recordings, those items shall be provided as soon as possible.

INTERLOCAL AUTHORITY

The Interlocal Act permits local governmental units to efficiently use of their powers by enabling them to provide joint or cooperative law enforcement services between agencies in a manner that will best aid the agencies and the citizens of the agencies served by such cooperative endeavors. In satisfaction of the requirement of the Interlocal Act; and in connection with this Agreement, the Parties agree the Agreement shall be approved pursuant to Utah Code §11-13-202.5 of the Interlocal Act after the Agreement has been reviewed and approved by a duly authorized attorney on behalf of each party. Furthermore, the parties agree and recognizes that no separate legal entity is created by the terms of this Agreement.

CONSIDERATION

The consideration for this Agreement consists of the mutual benefits and exchange of promises provided herein.

TERMINATION OF THE AGREEMENT

Either party may, at the party's sole discretion, terminate this Agreement at the end of the initial five-year period or at the end of any subsequent one-year renewal period with or without cause. Additionally, the failure of either party to comply with the terms of this Agreement shall constitute a breach of this Agreement. Thereafter, the non-compliance party shall have thirty (30) days after receipt of written notice of any breach to correct the conditions specified in the notice, or if the corrections cannot be made within the thirty (30) day period, within a reasonable time if corrective action is commenced with ten (10) days after receipt of the notice. Failure to correct the breach of conditions specified in the notice consistent with this timeframe will constitute cause to terminate this Agreement immediately thereafter.

RIGHTS AND REMEDIES

In the event of a breach, and after the lapse of the cure period as per above, beyond termination of the Agreement, the non-breaching party shall have all the rights and remedies available under

the laws of the State of Utah in effect. The rights and remedies of the parties shall not be mutually exclusive but shall be cumulative in all respects. The respective rights and obligations of the parties hereunder shall be enforceable in equity as well as at law or otherwise.

GOVERNING LAW, JURISDICTION, AND VENUE

All questions with respect to the construction of this Agreement, and all right and liability of the parties hereto shall be governed by the laws of the State of Utah. Jurisdiction and venue for the enforcement of this Agreement shall be found in the courts of Salt Lake County, State of Utah.

COSTS OF ENFORCEMENT

In the event of a breach of this Agreement, the non-breaching party shall be entitled to recover from the breaching party all of the non-breaching party's costs (including, but not limited to, court fees and expert witness costs) and attorneys' fees associated with the enforcement of this Agreement.

NOTICE

Any written notice that must or may be given relating to this Agreement shall be sufficient if mailed postage prepaid, registered or certified mail, in the United States mail addressed to a party at the address given above. In the case of the School District, notice shall be mailed to the attention of the Chief of GPD at the above address. In the case of City, notice shall be mailed to the attention of the South Salt Lake City Chief of Police at the above address. Either party may notify the other to designate a different address for mailing.

APPROPRIATION OF FUNDS

The Parties' obligations under this Agreement are expressly subject to the appropriation of funds by City and/or the School District's Board of Education. Discontinuation of appropriations necessary to perform the obligations of this contract may or may not necessitate termination of this Agreement at the end of the current annual contract cycle at the discretion of the parties.

INDEMNIFICATION

Both parties are governmental entities under the Governmental Immunity Act of Utah (the "Immunity Act"), Utah Code Ann. §§63G-7-101 to -904 (2011), as amended. Consistent with the terms of the Immunity Act, it is mutually agreed that each party is responsible and liable for its own wrongful or negligent acts, which it commits, or which are committed, by its agents,

officials, or employees. Neither Party waives any defenses otherwise available under the Immunity Act, nor does any party waive any limits of liability now or hereafter provided by law.

GENERAL PROVISIONS

1. Severability. If any condition, covenant, or other provision herein contained is held to be invalid or void by any court of competent jurisdiction, the same shall be deemed severable from the remainder of this Agreement and shall in no way affect any other covenant or condition herein contained. If such condition, covenant, or other provision shall be deemed invalid due to its scope or breadth, such provision shall be deemed valid to the extent of the scope or breadth permitted by law.
2. Entire Agreement. This Agreement contains the entire agreement between the parties. No promise, representation, warranty, or covenant not included in this Agreement has been or is relied upon by the parties. All prior understandings, negotiations, or agreements are merged herein and superseded hereby.
3. Amendments. This Agreement may be modified only by a writing signed by each of the parties hereto.
4. Covenants and Conditions. Each provision of this Agreement performable by City and the School District shall be deemed to be both a covenant and a condition.
5. Not Assignable. This Agreement is specific to the parties hereto and is therefore not assignable.
6. Binding Effect. This Agreement shall bind the parties and their respective successors and assigns.
7. Captions. The captions to the various Sections of this Agreement are for convenience and ease of reference only and do not define, limit, augment or describe the scope, content, or intent of this Agreement or any part or parts of this Agreement.
8. Time. Time is of the essence of each term, provision, and covenant of this Agreement.
9. Counterparts. This Agreement may be executed in two or more counterparts, each of which shall be deemed an original, but all of which shall constitute one instrument.
10. Gender and Number. The singular number includes the plural whenever the context so indicates. The neuter gender includes the feminine and masculine, the masculine includes the feminine and neuter, and the feminine includes the masculine and neuter, and each includes corporation, limited liability company, partnership, or other legal entity when the context so requires. The word "person" means person or persons or other entity or entities or any combination of persons and entities.
11. Waiver or Forbearance. No delay or omission in the exercise of any right or remedy by any party hereto shall impair such right or remedy or be construed as a waiver. Any

waiver of any breach must be in writing and shall not be a waiver of any other breach concerning the same or any other provision of this Agreement.

12. No Partnership, Joint Venture, or Third-Party Rights. Except as specifically set forth herein, nothing in this Agreement shall be construed as creating any partnership, joint, joint venture, or business arrangement among the parties hereto, nor any rights or benefits to third parties.

[Signature Page to Follow]

IN WITNESS THEREOF, the parties have signed and executed this SCHOOL RESOURCE OFFICER INTERLOCAL COOPERATION AGREEMENT on the dates listed below:

CITY OF SOUTH SALT LAKE

Dated this 18th day of July 2024

By: Cherie Wood *Cherie Wood*
South Salt Lake City Mayor

Attest: Ariel Andrus *Ariel Andrus*
South Salt Lake City Recorder

APPROVED AS TO FORM:

By: Brieanne Brass
South Salt Lake Deputy City Attorney

BOARD OF EDUCATION OF GRANITE SCHOOL DISTRICT

Dated this 18th day of July 2024

By: Benjamin Horsely _____
Superintendent

APPROVED AS TO FORM:

By: Douglas Larson _____
General Counsel

CJIS Security Policy_v5-8_20190601.pdf



Criminal Justice Information Services (CJIS) Security Policy

Version 5.8

06/01/2019

CJISD-ITS-DOC-08140-5.8



Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

EXECUTIVE SUMMARY

Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 1998. Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The Federal Information Security Management Act of 2002 provides further legal basis for the APB approved management, operational, and technical security requirements mandated to protect CJI and by extension the hardware, software and infrastructure required to enable the services provided by the criminal justice community.

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology. The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving business models. The Policy features modular sections enabling more frequent updates to address emerging threats and new security measures. The provided security criteria assists agencies with designing and implementing systems to meet a uniform level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.

The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus (SIB). Further, as use of criminal history record information for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in guiding the National Crime Prevention and Privacy Compact Council and State Compact Officers in the secure exchange of criminal justice records.

The Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The Policy empowers CSAs with the insight and ability to tune their security programs according to their risks, needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

CHANGE MANAGEMENT

Revision	Change Description	Created/Changed by	Date	Approved By
5	Policy Rewrite	Security Policy Working Group	2/9/2011	See Signature Page
5.1	Incorporate Calendar Year 2011 APB approved changes and administrative changes	CJIS ISO Program Office	7/13/2012	APB & Compact Council
5.2	Incorporate Calendar Year 2012 APB approved changes and administrative changes	CJIS ISO Program Office	8/9/2013	APB & Compact Council
5.3	Incorporate Calendar Year 2013 APB approved changes and administrative changes	CJIS ISO Program Office	8/4/2014	APB & Compact Council
5.4	Incorporate Calendar Year 2014 APB approved changes and administrative changes	CJIS ISO Program Office	10/6/2015	APB & Compact Council
5.5	Incorporate Calendar Year 2015 APB approved changes and administrative changes	CJIS ISO Program Office	6/1/2016	APB & Compact Council
5.6	Incorporate Calendar Year 2016 APB approved changes and administrative changes	CJIS ISO Program Office	6/5/2017	APB & Compact Council
5.7	Incorporate Calendar Year 2017 APB approved changes and administrative changes	CJIS ISO Program Office	08/16/2018	APB & Compact Council
5.8	Incorporate Calendar Year 2018 APB approved changes and administrative changes	CJIS ISO Program Office	06/01/2019	APB & Compact Council

SUMMARY OF CHANGES

Version 5.8

APB Approved Changes

1. **Section 3.2.2 CJIS Systems Officer (CSO):** change ‘2 d.’ to read consistent with other bullet appointment requirements, Fall 2018, APB#14, SA#5, Local Agency Security Officers (LASO) Training Requirement.
2. **Section 3.2.2 CJIS Systems Officer (CSO):** add requirement at ‘2 f.’ for LASO training, Fall 2018, APB#14, SA#5, Local Agency Security Officers (LASO) Training Requirement.
3. **Section 4.1 Criminal Justice Information (CJI):** add clarifying language to last paragraph, Fall 2018, APB#14, SA#7, SA Subcommittee Courts Task Force Recommendation.
4. **Section 5.2 Policy Area 2: Security Awareness Training:** add new introductory paragraph, Fall 2018, APB#14, SA#5, Local Agency Security Officers (LASO) Training Requirement.
5. **Section 5.2.1 Awareness Topics:** rename section to “Basic Security Awareness Training”, Fall 2018, APB#14, SA#5, Local Agency Security Officers (LASO) Training Requirement.
6. **Section 5.2.2 Security Training Records:** change section title to “LASO Training” and add new requirements, Fall 2018, APB#14, SA#5, Local Agency Security Officers (LASO) Training Requirement.
7. **Section 5.2.3 Security Training Records:** create new section from previous Section 5.2.2, Fall 2018, APB#14, SA#5, Local Agency Security Officers (LASO) Training Requirement.
8. **Section 5.6.2.1.1 Password:** add new introductory paragraph and note, Spring 2018, APB#17, SA#5, Adopting New Standards for Passwords from National Institute of Technologies (NIST) Special Publication 800-63D.
9. **Section 5.6.2.1.1.1 Basic Password Standards:** add new section number and title for existing password requirements, Spring 2018, APB#17, SA#5, Adopting New Standards for Passwords from National Institute of Technologies (NIST) Special Publication 800-63D.
10. **Section 5.6.2.1.1.2 Advanced Password Standards:** add new section and requirements, Spring 2018, APB#17, SA#5, Adopting New Standards for Passwords from National Institute of Technologies (NIST) Special Publication 800-63D.
11. **Section 5.10.1.3 Intrusion Detection Tools and Techniques:** add new introductory paragraph and requirements, Fall 2018, APB#14, SA#3, Intrusion Detection and Prevention Systems.
12. **Section 5.13.2 Mobile Device Management (MDM):** add exception to the MDM requirement for indirect access, Fall 2018, APB#14, SA#2, Mobile Device Management.
13. **Section 5.13.3 Wireless Device Risk Mitigations:** add language to bullets 6 and 7, Fall 2018, APB#14, SA#2, Mobile Device Management.
14. **Section 5.13.7.2 Advanced Authentication:** add language to relax requirement for indirect access, Fall 2018, APB#14, SA#2, Mobile Device Management.
15. **Section 5.13.7.2.1 Compensating Controls:** modify language to clarify requirements, Fall 2018, APB#14, SA#2, Mobile Device Management.

16. **Appendix A Terms and Definitions:** add definitions, “Hashing”, “Hash Value”, “Intrusion Detection”, “Intrusion Detection System”, “Intrusion Prevention”, “Intrusion Prevention System”, “Password Verifier”, “Salting”.
17. **Appendix B Acronyms:** “HIDS”, “HIPS”, “NIDS”, “NIPS”.

Administrative Changes¹

1. Appendix G.7 Incident Response Best Practices, add new appendix
2. Appendix G.8 Secure Coding Best Practices, add new appendix
3. Appendix K, General CJI Guidance, bullet k.: update language based on previous Section 5.12 changes (v5.7).

KEY TO APB APPROVED CHANGES (e.g. “Fall 2013, APB#11, SA#6, Topic Title”):

Fall 2013 – Advisory Policy Board cycle and year

APB## – Advisory Policy Board Topic number

SA## – Security and Access Subcommittee Topic number

Topic Title

¹ Administrative changes are vetted through the Security and Access Subcommittee and not the entire APB process.

TABLE OF CONTENTS

Executive Summary	i
Change Management	ii
Summary of Changes	iii
Table of Contents	v
List of Figures	x
1 Introduction	1
1.1 Purpose	1
1.2 Scope	1
1.3 Relationship to Local Security Policy and Other Policies	1
1.4 Terminology Used in This Document	2
1.5 Distribution of the CJIS Security Policy	2
2 CJIS Security Policy Approach	3
2.1 CJIS Security Policy Vision Statement	3
2.2 Architecture Independent	3
2.3 Risk Versus Realism	3
3 Roles and Responsibilities	4
3.1 Shared Management Philosophy	4
3.2 Roles and Responsibilities for Agencies and Parties	4
3.2.1 CJIS Systems Agencies (CSA)	5
3.2.2 CJIS Systems Officer (CSO)	5
3.2.3 Terminal Agency Coordinator (TAC)	6
3.2.4 Criminal Justice Agency (CJA)	6
3.2.5 Noncriminal Justice Agency (NCJA)	6
3.2.6 Contracting Government Agency (CGA)	7
3.2.7 Agency Coordinator (AC)	7
3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)	7
3.2.9 Local Agency Security Officer (LASO)	8
3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)	8
3.2.11 Repository Manager	9
3.2.12 Compact Officer	9
4 Criminal Justice Information and Personally Identifiable Information	10
4.1 Criminal Justice Information (CJI)	10
4.1.1 Criminal History Record Information (CHRI)	10
4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information	11
4.2.1 Proper Access, Use, and Dissemination of CHRI	11
4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information	11
4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information	11
4.2.3.1 For Official Purposes	11
4.2.3.2 For Other Authorized Purposes	12
4.2.3.3 CSO Authority in Other Circumstances	12
4.2.4 Storage	12
4.2.5 Justification and Penalties	12

4.2.5.1	Justification	12
4.2.5.2	Penalties	12
4.3	Personally Identifiable Information (PII).....	12
5	Policy and Implementation	14
5.1	Policy Area 1: Information Exchange Agreements	15
5.1.1	Information Exchange	15
5.1.1.1	Information Handling.....	15
5.1.1.2	State and Federal Agency User Agreements	15
5.1.1.3	Criminal Justice Agency User Agreements	16
5.1.1.4	Interagency and Management Control Agreements	16
5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum.....	16
5.1.1.6	Agency User Agreements	17
5.1.1.7	Outsourcing Standards for Channelers	17
5.1.1.8	Outsourcing Standards for Non-Channelers	18
5.1.2	Monitoring, Review, and Delivery of Services	18
5.1.2.1	Managing Changes to Service Providers	18
5.1.3	Secondary Dissemination.....	18
5.1.4	Secondary Dissemination of Non-CHRI CJI	18
5.2	Policy Area 2: Security Awareness Training.....	20
5.2.1	Basic Security Awareness Training	20
5.2.1.1	Level One Security Awareness Training	20
5.2.1.2	Level Two Security Awareness Training	20
5.2.1.3	Level Three Security Awareness Training	21
5.2.1.4	Level Four Security Awareness Training	21
5.2.2	LASO Training.....	22
5.2.3	Security Training Records.....	22
5.3	Policy Area 3: Incident Response	24
5.3.1	Reporting Security Events.....	24
5.3.1.1	Reporting Structure and Responsibilities.....	24
5.3.1.1.1	FBI CJIS Division Responsibilities	24
5.3.1.1.2	CSA ISO Responsibilities.....	24
5.3.2	Management of Security Incidents.....	25
5.3.2.1	Incident Handling.....	25
5.3.2.2	Collection of Evidence.....	25
5.3.3	Incident Response Training.....	25
5.3.4	Incident Monitoring.....	25
5.4	Policy Area 4: Auditing and Accountability.....	27
5.4.1	Auditable Events and Content (Information Systems).....	27
5.4.1.1	Events.....	27
5.4.1.1.1	Content.....	28
5.4.2	Response to Audit Processing Failures	28
5.4.3	Audit Monitoring, Analysis, and Reporting.....	28
5.4.4	Time Stamps.....	28
5.4.5	Protection of Audit Information	28
5.4.6	Audit Record Retention.....	28
5.4.7	Logging NCIC and III Transactions.....	29

5.5	Policy Area 5: Access Control.....	30
5.5.1	Account Management	30
5.5.2	Access Enforcement.....	30
5.5.2.1	Least Privilege	31
5.5.2.2	System Access Control	31
5.5.2.3	Access Control Criteria.....	31
5.5.2.4	Access Control Mechanisms.....	31
5.5.3	Unsuccessful Login Attempts	32
5.5.4	System Use Notification.....	32
5.5.5	Session Lock	32
5.5.6	Remote Access	33
5.5.6.1	Personally Owned Information Systems.....	33
5.5.6.2	Publicly Accessible Computers	33
5.6	Policy Area 6: Identification and Authentication	35
5.6.1	Identification Policy and Procedures.....	35
5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges	35
5.6.2	Authentication Policy and Procedures	35
5.6.2.1	Standard Authenticators.....	36
5.6.2.1.1	Password	36
5.6.2.1.2	Personal Identification Number (PIN)	38
5.6.2.1.3	One-time Passwords (OTP)	38
5.6.2.2	Advanced Authentication.....	38
5.6.2.2.1	Advanced Authentication Policy and Rationale	39
5.6.2.2.2	Advanced Authentication Decision Tree	39
5.6.3	Identifier and Authenticator Management	41
5.6.3.1	Identifier Management.....	41
5.6.3.2	Authenticator Management.....	42
5.6.4	Assertions	42
5.7	Policy Area 7: Configuration Management	48
5.7.1	Access Restrictions for Changes	48
5.7.1.1	Least Functionality.....	48
5.7.1.2	Network Diagram.....	48
5.7.2	Security of Configuration Documentation	48
5.8	Policy Area 8: Media Protection.....	49
5.8.1	Media Storage and Access	49
5.8.2	Media Transport	49
5.8.2.1	Digital Media during Transport	49
5.8.2.2	Physical Media in Transit	49
5.8.3	Digital Media Sanitization and Disposal.....	49
5.8.4	Disposal of Physical Media.....	49
5.9	Policy Area 9: Physical Protection	51
5.9.1	Physically Secure Location	51
5.9.1.1	Security Perimeter.....	51
5.9.1.2	Physical Access Authorizations	51
5.9.1.3	Physical Access Control	51

5.9.1.4	Access Control for Transmission Medium	51
5.9.1.5	Access Control for Display Medium	51
5.9.1.6	Monitoring Physical Access	52
5.9.1.7	Visitor Control	52
5.9.1.8	Delivery and Removal	52
5.9.2	Controlled Area	52
5.10	Policy Area 10: System and Communications Protection and Information Integrity	53
5.10.1	Information Flow Enforcement	53
5.10.1.1	Boundary Protection	53
5.10.1.2	Encryption	54
5.10.1.2.1	Encryption for CJI in Transit	54
5.10.1.2.2	Encryption for CJI at Rest	55
5.10.1.2.3	Public Key Infrastructure (PKI) Technology	55
5.10.1.3	Intrusion Detection Tools and Techniques	55
5.10.1.4	Voice over Internet Protocol	56
5.10.1.5	Cloud Computing	56
5.10.2	Facsimile Transmission of CJI	57
5.10.3	Partitioning and Virtualization	57
5.10.3.1	Partitioning	57
5.10.3.2	Virtualization	58
5.10.4	System and Information Integrity Policy and Procedures	58
5.10.4.1	Patch Management	58
5.10.4.2	Malicious Code Protection	59
5.10.4.3	Spam and Spyware Protection	59
5.10.4.4	Security Alerts and Advisories	59
5.10.4.5	Information Input Restrictions	60
5.11	Policy Area 11: Formal Audits	61
5.11.1	Audits by the FBI CJIS Division	61
5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	61
5.11.1.2	Triennial Security Audits by the FBI CJIS Division	61
5.11.2	Audits by the CSA	61
5.11.3	Special Security Inquiries and Audits	62
5.11.4	Compliance Subcommittees	62
5.12	Policy Area 12: Personnel Security	63
5.12.1	Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI	63
5.12.2	Personnel Termination	64
5.12.3	Personnel Transfer	64
5.12.4	Personnel Sanctions	64
5.13	Policy Area 13: Mobile Devices	66
5.13.1	Wireless Communications Technologies	66
5.13.1.1	802.11 Wireless Protocols	66
5.13.1.2	Cellular Devices	67
5.13.1.2.1	Cellular Service Abroad	68
5.13.1.2.2	Voice Transmissions Over Cellular Devices	68
5.13.1.3	Bluetooth	68

5.13.1.4 Mobile Hotspots.....	68
5.13.2 Mobile Device Management (MDM)	69
5.13.3 Wireless Device Risk Mitigations	69
5.13.4 System Integrity	70
5.13.4.1 Patching/Updates	70
5.13.4.2 Malicious Code Protection.....	70
5.13.4.3 Personal Firewall	70
5.13.5 Incident Response	71
5.13.6 Access Control	71
5.13.7 Identification and Authentication.....	71
5.13.7.1 Local Device Authentication	71
5.13.7.2 Advanced Authentication.....	72
5.13.7.2.1 Compensating Controls.....	72
5.13.7.3 Device Certificates.....	72
Appendices.....	A-1
Appendix A Terms and Definitions	A-1
Appendix B Acronyms	B-1
Appendix C Network Topology Diagrams	C-1
Appendix D Sample Information Exchange Agreements	D-1
D.1 CJIS User Agreement	D-1
D.2 Management Control Agreement.....	D-9
D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding.....	D-10
D.4 Interagency Connection Agreement	D-16
Appendix E Security Forums and Organizational Entities.....	E-1
Appendix F Sample Forms.....	F-1
F.1 Security Incident Response Form	F-2
Appendix G Best practices	G-1
G.1 Virtualization	G-1
G.2 Voice over Internet Protocol.....	G-4
G.3 Cloud Computing.....	G-15
G.4 Mobile Appendix	G-32
G.5 Administrator Accounts for Least Privilege and Separation of Duties.....	G-53
G.6 Encryption.....	G-66
G.7 Incident Response	G-1
G.8 Secure Coding.....	G-1
Appendix H Security Addendum	H-1
Appendix I References	I-1
Appendix J Noncriminal Justice Agency Supplemental Guidance	J-1
Appendix K Criminal Justice Agency Supplemental Guidance	K-1

LIST OF FIGURES

Figure 1 – Overview Diagram of Strategic Functions and Policy Components	4
Figure 2 – Dissemination of restricted and non-restricted NCIC data.....	13
Figure 3 – Information Exchange Agreements Implemented by a Local Police Department	19
Figure 4 – Security Awareness Training Use Cases	22
Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department	26
Figure 6 – Local Police Department's Use of Audit Logs	29
Figure 7 – A Local Police Department's Access Controls	34
Figure 8 – Advanced Authentication Use Cases.....	42
Figure 9 – Authentication Decision for Known Location	46
Figure 10 – Authentication Decision for Unknown Location	47
Figure 11 – A Local Police Department's Configuration Management Controls	48
Figure 12 – A Local Police Department's Media Management Policies.....	50
Figure 13 – A Local Police Department's Physical Protection Measures.....	52
Figure 14 – System and Communications Protection and Information Integrity Use Cases.....	60
Figure 15 – The Audit of a Local Police Department.....	62
Figure 16 – A Local Police Department's Personnel Security Controls	64

1 INTRODUCTION

This section details the purpose of this document, its scope, relationship to other information security policies, and its distribution constraints.

1.1 Purpose

The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council).

1.2 Scope

At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The CJIS Security Policy provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CJI data for noncriminal justice purposes are also governed by the standards and rules promulgated by the Compact Council.

1.3 Relationship to Local Security Policy and Other Policies

The CJIS Security Policy may be used as the sole security policy for the agency. The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJIS Security Policy areas can be developed for the security program in general, and for a particular information system, when required.

This document is a compendium of applicable policies in providing guidance on the minimum security controls and requirements needed to access FBI CJIS information and services. These policies include presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions. State, local, and Tribal CJA may implement more stringent policies

and requirements. Appendix I contains the references while Appendix E lists the security forums and organizational entities referenced in this document.

1.4 Terminology Used in This Document

The following terms are used interchangeably throughout this document:

- **Agency and Organization:** The two terms in this document refer to any entity that submits or receives information, by any means, to/from FBI CJIS systems or services.
- **Information and Data:** Both terms refer to CJI.
- **System, Information System, Service, or named applications like NCIC:** all refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections.
- **References/Citations/Directives:** Appendix I contains all of the references used in this Policy and may contain additional sources that could apply to any section.

Appendix A and B provide an extensive list of the terms and acronyms.

1.5 Distribution of the CJIS Security Policy

The CJIS Security Policy, version 5.0 and later, is a publicly available document and may be posted and shared without restrictions.

2 CJIS SECURITY POLICY APPROACH

The CJIS Security Policy represents the shared responsibility between FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJI. The Policy provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives.

2.1 CJIS Security Policy Vision Statement

The executive summary of this document describes the vision in terms of business needs for confidentiality, integrity, and availability of information. The APB collaborates with the FBI CJIS Division to ensure that the Policy remains updated to meet evolving business, technology and security needs.

2.2 Architecture Independent

Due to advancing technology and evolving business models, the FBI CJIS Division is transitioning from legacy stovepipe systems and moving toward a flexible services approach. Systems such as National Crime Information Center (NCIC), National Instant Criminal Background Check System (NICS), and Next Generation Identification (NGI) will continue to evolve and may no longer retain their current system platforms, hardware, or program name. However, the data and services provided by these systems will remain stable.

The CJIS Security Policy looks at the data (information), services, and protection controls that apply regardless of the implementation architecture. Architectural independence is not intended to lessen the importance of systems, but provide for the replacement of one technology with another while ensuring the controls required to protect the information remain constant. This objective and conceptual focus on security policy areas provide the guidance and standards while avoiding the impact of the constantly changing landscape of technical innovations. The architectural independence of the Policy provides agencies with the flexibility for tuning their information security infrastructure and policies to reflect their own environments.

2.3 Risk Versus Realism

Every “shall” statement contained within the CJIS Security Policy has been scrutinized for risk versus the reality of resource constraints and real-world application. The purpose of the CJIS Security Policy is to establish the minimum security requirements; therefore, individual agencies are encouraged to implement additional controls to address agency specific risks. Each agency faces risk unique to that agency. It is quite possible that several agencies could encounter the same type of risk however depending on resources would mitigate that risk differently. In that light, a risk-based approach can be used when implementing requirements.

3 ROLES AND RESPONSIBILITIES

3.1 Shared Management Philosophy

In the scope of information security, the FBI CJIS Division employs a shared management philosophy with federal, state, local, and tribal law enforcement agencies. Although an advisory policy board for the NCIC has existed since 1969, the Director of the FBI established the CJIS APB in March 1994 to enable appropriate input and recommend policy with respect to CJIS services. Through the APB and its Subcommittees and Working Groups, consideration is given to the needs of the criminal justice and law enforcement community regarding public policy, statutory and privacy aspects, as well as national security relative to CJIS systems and information. The APB represents federal, state, local, and tribal law enforcement and criminal justice agencies throughout the United States, its territories, and Canada.

The FBI has a similar relationship with the Compact Council, which governs the interstate exchange of criminal history records for noncriminal justice purposes. The Compact Council is mandated by federal law to promulgate rules and procedures for the use of the Interstate Identification Index (III) for noncriminal justice purposes. To meet that responsibility, the Compact Council depends on the CJIS Security Policy as the definitive source for standards defining the security and privacy of records exchanged with noncriminal justice practitioners.

3.2 Roles and Responsibilities for Agencies and Parties

It is the responsibility of all agencies covered under this Policy to ensure the protection of CJI between the FBI CJIS Division and its user community. The following figure provides an abstract representation of the strategic functions and roles such as governance and operations.

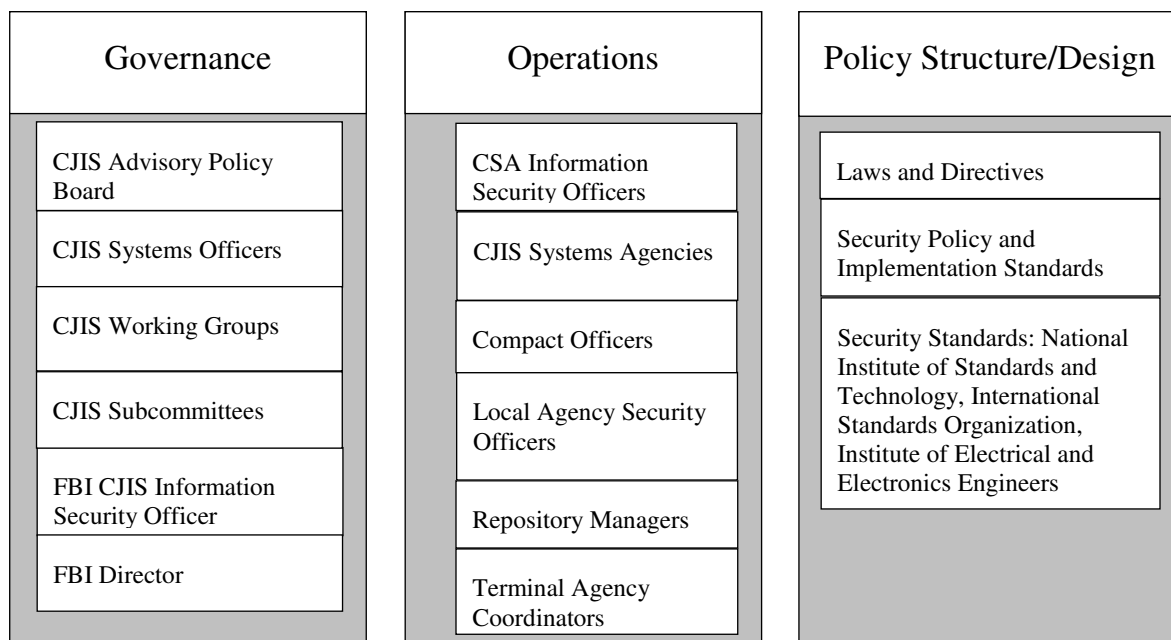


Figure 1 – Overview Diagram of Strategic Functions and Policy Components

This section provides a description of the following entities and roles:

1. CJIS Systems Agency.
2. CJIS Systems Officer.
3. Terminal Agency Coordinator.
4. Criminal Justice Agency.
5. Noncriminal Justice Agency.
6. Contracting Government Agency.
7. Agency Coordinator.
8. CJIS Systems Agency Information Security Officer.
9. Local Agency Security Officer.
10. FBI CJIS Division Information Security Officer.
11. Repository Manager.
12. Compact Officer.

3.2.1 CJIS Systems Agencies (CSA)

The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels. The head of each CSA shall appoint a CJIS Systems Officer (CSO). The CSA may impose more stringent protection measures than outlined in this document. Such decisions shall be documented and kept current.

3.2.2 CJIS Systems Officer (CSO)

The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. Pursuant to the Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. The CSO may delegate responsibilities to subordinate agencies. The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJI.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
 - a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
 - b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.

- c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.
 - d. Ensure the designation of a Terminal Agency Coordinator (TAC) within each agency with devices accessing CJIS systems.
 - e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).
 - f. Ensure each LASO receives enhanced security awareness training (ref. Section 5.2).
 - g. Approve access to FBI CJIS systems.
 - h. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.
 - i. Perform other related duties outlined by the user agreements with the FBI CJIS Division.
3. Outsourcing of Criminal Justice Functions
- a. Responsibility for the management of the approved security requirements shall remain with the CJA. Security control includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJI; and to guarantee the priority service needed by the criminal justice community.
 - b. Responsibility for the management control of network security shall remain with the CJA. Management control of network security includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of circuits and network equipment used to transmit CJI; and to guarantee the priority service as determined by the criminal justice community.

3.2.3 Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

3.2.4 Criminal Justice Agency (CJA)

A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

3.2.5 Noncriminal Justice Agency (NCJA)

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

3.2.6 Contracting Government Agency (CGA)

A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC)

An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the FBI.

3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.

2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)

The FBI CJIS ISO shall:

1. Maintain the CJIS Security Policy.
2. Disseminate the FBI Director approved CJIS Security Policy.
3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.

3.2.11 Repository Manager

The State Identification Bureau (SIB) Chief, i.e. Repository Manager or Chief Administrator, is the designated manager of the agency having oversight responsibility for a state's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

3.2.12 Compact Officer

Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. Case/Incident History—information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules. CJI introduced into the court system pursuant to a judicial proceeding and that can be released to the public via a public records request is not subject to the CJIS Security Policy.

4.1.1 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI), sometimes informally referred to as “restricted data”, is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.

4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information

This section describes the requirements for the access, use and dissemination of CHRI, NCIC restricted files information, and NCIC non-restricted files information.

4.2.1 Proper Access, Use, and Dissemination of CHRI

Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information

The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:

1. Gang Files
2. Known or Appropriately Suspected Terrorist Files
3. Supervised Release Files
4. National Sex Offender Registry Files
5. Historical Protection Order Files of the NCIC
6. Identity Theft Files
7. Protective Interest Files
8. Person With Information (PWI) data in the Missing Person Files
9. Violent Person File
10. NICS Denied Transactions File

The remaining NCIC files are considered non-restricted files.

4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information

4.2.3.1 For Official Purposes

NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with

the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

4.2.3.2 For Other Authorized Purposes

NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially.

A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.

4.2.3.3 CSO Authority in Other Circumstances

If no federal, state or local law or policy prohibition exists, the CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted file information.

4.2.4 Storage

When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. See Section 5.9 for physical security controls.

4.2.5 Justification and Penalties

4.2.5.1 Justification

In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.

4.2.5.2 Penalties

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

4.3 Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for

example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

Figure 2 – Dissemination of restricted and non-restricted NCIC data

A citizen of Springfield went to the Springfield Police Department to request whether his new neighbor, who had been acting suspiciously, had an outstanding warrant. The Springfield Police Department ran an NCIC persons inquiry, which produced a response that included a Wanted Person File (non-restricted file) record and a Known or Appropriately Suspected Terrorist File (restricted file) record. The Springfield Police Department advised the citizen of the outstanding warrant, but did not disclose any information concerning the subject being a known or appropriately suspected terrorist.

5 POLICY AND IMPLEMENTATION

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances. The policy areas are:

- Policy Area 1—Information Exchange Agreements
- Policy Area 2—Security Awareness Training
- Policy Area 3—Incident Response
- Policy Area 4—Auditing and Accountability
- Policy Area 5—Access Control
- Policy Area 6—Identification and Authentication
- Policy Area 7—Configuration Management
- Policy Area 8—Media Protection
- Policy Area 9—Physical Protection
- Policy Area 10—Systems and Communications Protection and Information Integrity
- Policy Area 11—Formal Audits
- Policy Area 12—Personnel Security
- Policy Area 13—Mobile Devices

5.1 Policy Area 1: Information Exchange Agreements

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

5.1.1 Information Exchange

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.

5.1.1.1 Information Handling

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including – but not limited to – employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

5.1.1.2 State and Federal Agency User Agreements

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA

or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.

5.1.1.3 Criminal Justice Agency User Agreements

Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:

1. Audit.
2. Dissemination.
3. Hit confirmation.
4. Logging.
5. Quality Assurance (QA).
6. Screening (Pre-Employment).
7. Security.
8. Timeliness.
9. Training.
10. Use of the system.
11. Validation.

5.1.1.4 Interagency and Management Control Agreements

A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an interagency agreement. An example of an NCJA (government) is a city information technology (IT) department.

5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum

The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security

Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

5.1.1.6 Agency User Agreements

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

5.1.1.7 Outsourcing Standards for Channelers

Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact

Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.

Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.1.8 Outsourcing Standards for Non-Channelers

Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.2 Monitoring, Review, and Delivery of Services

As specified in the interagency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.

5.1.2.1 Managing Changes to Service Providers

Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

5.1.3 Secondary Dissemination

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

5.1.4 Secondary Dissemination of Non-CHRI CJI

If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.

Figure 3 – Information Exchange Agreements Implemented by a Local Police Department

A local police department executed a Memorandum of Understanding (MOU) for the interface with their state CSA. The local police department also executed an MOU (which included an MCA) with the county information technology (IT) department for the day-to-day operations of their criminal-justice infrastructure. The county IT department, in turn, outsourced operations to a local vendor who signed the CJIS Security Addendum.

5.2 Policy Area 2: Security Awareness Training

Security training is key to the human element of information security. All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.

5.2.1 Basic Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. The CSO/SIB Chief may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

5.2.1.1 Level One Security Awareness Training

At a minimum, the following topics shall be addressed as baseline security awareness training for all personnel who have unescorted access to a physically secure location:

1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.
2. Implications of noncompliance.
3. Incident response (Identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

5.2.1.2 Level Two Security Awareness Training

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Media protection.
2. Protect information subject to confidentiality concerns — hardcopy through destruction.
3. Proper handling and marking of CJI.
4. Threats, vulnerabilities, and risks associated with handling of CJI.
5. Social engineering.
6. Dissemination and destruction.

5.2.1.3 Level Three Security Awareness Training

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJIS:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.
2. Password usage and management—including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code.
4. Unknown e-mail/attachments.
5. Web usage—allowed versus prohibited; monitoring of user activity.
6. Spam.
7. Physical Security—increases in risks to systems and data.
8. Handheld device security issues—address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
10. Laptop security—address both physical and information security issues.
11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
12. Access control issues—address least privilege and separation of duties.
13. Individual accountability—explain what this means in the agency.
14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating “shoulder surfing”), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

5.2.1.4 Level Four Security Awareness Training

In addition to 5.2.1.1, 5.2.1.2, and 5.1.2.3 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
2. Data backup and storage—centralized or decentralized approach.

3. Timely application of system patches—part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.

5.2.2 LASO Training

LASO training shall be required prior to assuming duties but no later than six months after initial assignment, and annually thereafter.

At a minimum, the following topics shall be addressed as enhanced security awareness training for a LASO:

1. The roles and responsibilities listed in CJIS Security Policy Section 3.2.9.
2. Additional state/local/tribal/federal agency LASO roles and responsibilities.
3. Summary of audit findings from previous state audits of local agencies.
4. Findings from the last FBI CJIS Division audit of the CSA.
5. Most recent changes to the CJIS Security Policy.

5.2.3 Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB Chief/Compact Officer. Maintenance of training records can be delegated to the local level.

Figure 4 – Security Awareness Training Use Cases

Use Case 1 - Security Awareness Training Program Implementation by a Local Police Department

A local police department with a staff of 20 sworn criminal justice professionals and 15 support personnel worked with a vendor to develop role-specific security-awareness training, and required all staff to complete this training upon assignment and every two years thereafter. The local police department scheduled the sworn law-enforcement training to coincide with their NCIC certification training. The vendor maintained the training records for the police department's entire staff, and provided reporting to the department to help it ensure compliance with the CJIS Security Policy.

Use Case 2 - Level One Security Awareness Training

A local police department hires custodial staff that will have physical access throughout the PD (a physically secure location) after normal business hours to clean the facility. These personnel have unescorted access to a physically secure location and therefore must be given the baseline security awareness training on all the topics identified in CSP Section 5.2.1.1 Level One Security Awareness Training.

Use Case 3 – Level Two Security Awareness Training

A school district maintains a locked file cabinet with hard copies of background check results of all teachers and employees which may include CJI (CHRI). Only authorized personnel who have the

ability to open the cabinet are required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1 and 5.2.1.2.

Use Case 4 – Level Three Security Awareness Training

A County Sheriff's Office has employed a number of dispatchers. Part of the function of these dispatchers is to run CJI queries at the request of the Sheriff and deputies. As part of their daily duties, the dispatchers have access to CJI both logically (running queries) and physically (printed copies of reports containing CJI). These dispatchers are entrusted with direct access to CJI and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, and 5.2.1.3.

Use Case 5 – Level Four Security Awareness Training

The State Police has hired a number of system and network administrator personnel to help bolster security of the state network. Part of their daily duties may include creating accounts for new personnel, implementing security patches for existing systems, creating backups of existing systems, and implementing access controls throughout the network. These administrators have privileged access to CJI and CJI-processing systems, and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, 5.2.1.3, and 5.2.1.4.

5.3 Policy Area 3: Incident Response

The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of a CJI-related incident to the FBI CJIS ISO.

Refer to Section 5.13.5 for additional incident response requirements related to mobile devices used to access CJI.

5.3.1 Reporting Security Events

The agency shall promptly report incident information to appropriate authorities. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

5.3.1.1 Reporting Structure and Responsibilities

5.3.1.1.1 FBI CJIS Division Responsibilities

The FBI CJIS Division shall:

1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
4. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
5. Track all reported incidents and/or trends.
6. Monitor the resolution of all incidents.

5.3.1.1.2 CSA ISO Responsibilities

The CSA ISO shall:

1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
6. Act as a single POC for their jurisdictional area for requesting incident response assistance.

5.3.2 Management of Security Incidents

A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

5.3.2.1 Incident Handling

The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

5.3.2.2 Collection of Evidence

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

5.3.3 Incident Response Training

The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.

5.3.4 Incident Monitoring

The agency shall track and document security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department

A state ISO received a notification from a local police department that suspicious network activity from a known botnet was detected on their network. The state ISO began the process of collecting all pertinent information about this incident, e.g. incident date/time, points-of-contact, systems affected, nature of the incident, actions taken, etc. and requested that the local police department confirm that their malware signatures were up to date. The state ISO contacted both the FBI CJIS ISO and state CSO to relay the preliminary details of this incident. The FBI CJIS ISO instructed the involved parties to continue their investigation and to submit an incident response form once all the information had been gathered. The FBI CJIS ISO contacted the lead for the FBI CSIRC to inform them that an incident response form was forthcoming. The state ISO gathered the remainder of the information from the local police department and submitted a completed incident response form to the FBI CJIS ISO who subsequently provided it to the FBI CSIRC. The FBI CSIRC notified the Department of Justice Computer Incident Response Team (DOJCIRT). The state ISO continued to monitor the situation, passing relevant details to the FBI CJIS ISO, ultimately determining that the botnet was eliminated from the local police department's infrastructure. Subsequent investigations determined that the botnet was restricted to the department's administrative infrastructure and thus no CJI was compromised.

5.4 Policy Area 4: Auditing and Accountability

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

Refer to Section 5.13.6 for additional audit requirements related to mobile devices used to access CJI.

5.4.1 Auditable Events and Content (Information Systems)

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems.

The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
 - a. access permission on a user account, file, directory or other system resource;
 - b. create permission on a user account, file, directory or other system resource;
 - c. write permission on a user account, file, directory or other system resource;
 - d. delete permission on a user account, file, directory or other system resource;
 - e. change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts (i.e. root, Oracle, DBA, admin, etc.).
5. Successful and unsuccessful attempts for users to:
 - a. access the audit log file;

- b. modify the audit log file;
- c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

5.4.2 Response to Audit Processing Failures

The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

5.4.3 Audit Monitoring, Analysis, and Reporting

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

5.4.4 Time Stamps

The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

5.4.5 Protection of Audit Information

The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

5.4.6 Audit Record Retention

The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for

example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

5.4.7 Logging NCIC and III Transactions

A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.

Figure 6 – Local Police Department's Use of Audit Logs

A state CSO contacted a local police department regarding potentially inappropriate use of CHRI that was retrieved using the local department's ORI. The state CSO requested all relevant information from the police department to reconcile state NCIC and III logs against local police department logs. The police department provided the combination of their CJI processing application's logs with relevant operating system and network infrastructure logs to help verify the identity of the users conducting these queries. The review of these logs substantiated the CSO's suspicion.

5.5 Policy Area 5: Access Control

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

Refer to Section 5.13.6 for additional access control requirements related to mobile devices used to access CJI.

5.5.1 Account Management

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The agency responsible for account creation shall be notified when:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

5.5.2 Access Enforcement

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

5.5.2.1 Least Privilege

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.

Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.

5.5.2.2 System Access Control

Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to:

1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.
2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

5.5.2.3 Access Control Criteria

Agencies shall control access to CJI based on one or more of the following:

1. Job assignment or function (i.e., the role) of the user seeking access.
2. Physical location.
3. Logical location.
4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
5. Time-of-day and day-of-week/month restrictions.

5.5.2.4 Access Control Mechanisms

When setting up access controls, agencies shall use one or more of the following mechanisms:

1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.
2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.

3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. Follow the guidance in Section 5.10.1.2 for encryption requirements if encryption of stored information is employed as an access enforcement mechanism.
4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

5.5.3 Unsuccessful Login Attempts

Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.

5.5.4 System Use Notification

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is accessing a restricted information system.
2. System usage may be monitored, recorded, and subject to audit.
3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

1. the system use information is available and when appropriate, is displayed before granting access;
2. any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and
3. the notice given to public users of the information system includes a description of the authorized uses of the system.

5.5.5 Session Lock

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall

directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e. receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.

5.5.6 Remote Access

The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system.

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

1. The session shall be monitored at all times by an authorized escort
2. The escort shall be familiar with the system/area in which the work is being performed.
3. The escort shall have the ability to end the session at any time.
4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

5.5.6.1 Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.

This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

5.5.6.2 Publicly Accessible Computers

Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Figure 7 – A Local Police Department’s Access Controls

A local police department purchased a new computer-assisted dispatch (CAD) system that integrated with their state CSA’s CJI interfaces. In doing so, the police department employed least-privilege practices to ensure that its employees were only given those privileges needed to perform their jobs, and as such, excluding IT administrators, employees had only non-administrative privileges on all equipment they used. The police department also used ACLs in the operating systems to control access to the CAD client’s executables. The CAD system used internal role-based access controls to ensure only those users that needed access to CJI were given it. The police department performed annual audits of user accounts on all systems under their control including remote access mechanisms, operating systems, and the CAD system to ensure all accounts were in valid states. The police department implemented authentication-failure account lockouts, system use notification via login banners, and screen-saver passwords on all equipment that processes CJI.

5.6 Policy Area 6: Identification and Authentication

The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.

5.6.1 Identification Policy and Procedures

Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges

An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.

Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.

Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

5.6.2 Authentication Policy and Procedures

Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI.

Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not

further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.

5.6.2.1 Standard Authenticators

Authenticators are (the something you know, something you are, or something you have) part of the identification and authentication process. Examples of standard authenticators include passwords, hard or soft tokens, biometrics, one-time passwords (OTP) and personal identification numbers (PIN). Users shall not be allowed to use the same password or PIN in the same logon sequence.

5.6.2.1.1 Password

When agencies use a password as an authenticator for an individual's unique ID, they shall use the basic password standards in 5.6.2.1.1.1, OR follow the advanced password standards in 5.6.2.1.1.2.

NOTE: There is no option to combine or select particular options between the two separate lists below.

5.6.2.1.1.1 Basic Password Standards

When agencies elect to follow the basic password standards, passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

5.6.2.1.1.2 Advanced Password Standards

When agencies elect to follow the advanced password standards, follow the guidance below:

1. Passwords shall be a minimum of twenty (20) characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).
2. Password Verifiers shall not permit the use of a stored "hint" for forgotten passwords and/or prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing a password.
3. Verifiers shall maintain a list of "banned passwords" that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:

- a. Passwords obtained from previous breach corpuses
 - b. Dictionary words
 - c. Repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’)
 - d. Context-specific words, such as the name of the service, the username, and derivatives thereof
4. When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the “banned passwords” list.
5. If the chosen password is found to be part of a “banned passwords” list, the Verifier shall:
 - a. Advise the subscriber that they need to select a different password,
 - b. Provide the reason for rejection, and
 - c. Require the subscriber to choose a different password.
6. Verifiers shall limit the number of failed authentication attempts that can be made as described in Section 5.5.3 Unsuccessful Login Attempts.
7. Verifiers shall force a password change if there is evidence of authenticator compromise or every 365 days from the last password change.
8. Verifiers shall use approved encryption and an authenticated protected channel when requesting passwords to protect against eavesdropping and Man-in-the-Middle (MitM) attacks.
9. Verifiers shall store passwords in a manner that is resistant to offline attacks by salting and hashing the password using a one-way key derivation function when stored.
 - a. The salt shall be at least 32 bits in length.
 - b. The salt shall be chosen arbitrarily so as to minimize salt value collisions among stored hashes.

Note: Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive.
10. For each subscriber, Verifiers shall protect stored salt and resulting hash values using a password or PIN.

5.6.2.1.2 Personal Identification Number (PIN)

When agencies implement the use of a PIN as a standard authenticator, the PIN attributes shall follow the guidance in section 5.6.2.1.1 (password). When agencies utilize a PIN in conjunction with a certificate or a token (e.g. key fob with rolling numbers) for the purpose of advanced authentication, agencies shall follow the PIN attributes described below. For example: A user certificate is installed on a smartphone for the purpose of advanced authentication (AA). As the user invokes that certificate, a PIN meeting the below attributes shall be used to access the certificate for the AA process.

1. Be a minimum of six (6) digits
2. Have no repeating digits (i.e., 112233)
3. Have no sequential patterns (i.e., 123456)
4. Not be the same as the Userid.
5. Expire within a maximum of 365 calendar days.
 - a. If a PIN is used to access a soft certificate which is the second factor of authentication, AND the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 365 day expiration requirement can be waived by the CSO.
6. Not be identical to the previous three (3) PINs.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.

EXCEPTION: When a PIN is used for local device authentication, the only requirement is that it be a minimum of six (6) digits.

5.6.2.1.3 One-time Passwords (OTP)

One-time passwords are considered a “something you have” token for authentication. Examples include bingo cards, hard or soft tokens, and out-of-band tokens (i.e. OTP received via a text message).

When agencies implement the use of an OTP as an authenticator, the OTP shall meet the requirements described below.

1. Be a minimum of six (6) randomly generated characters
2. Be valid for a single session
3. If not used, expire within a maximum of five (5) minutes after issuance

5.6.2.2 Advanced Authentication

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.), or “Risk-based Authentication” that includes a software token element comprised of a number of factors, such as

network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

When user-based certificates are used for authentication purposes, they shall:

1. Be specific to an individual user and not to a particular device.
2. Prohibit multiple users from utilizing the same certificate.
3. Require the user to “activate” that certificate for each use in some manner (e.g., passphrase or user-specific PIN).

5.6.2.2.1 Advanced Authentication Policy and Rationale

The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions. The CSO will make the final determination of whether access is considered indirect.

The intent of AA is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

EXCEPTION:

AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. **EXAMPLES:**

1. A user, irrespective of his/her location, accesses the LEEP portal. The LEEP has AA built into its services and requires AA prior to granting access. AA is required.
2. A user, irrespective of their location, accesses a State’s portal through which access to CJI is facilitated. The State Portal has AA built into its processes and requires AA prior to granting access. AA is required.

5.6.2.2.2 Advanced Authentication Decision Tree

The following AA Decision Tree, coupled with figures 9 and 10 below, assists decision makers in determining whether or not AA is required.

1. Can request’s physical originating location be determined?
If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 2.
 - a. The IP address is attributed to a physical structure; or

- b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure.

If neither (a) or (b) above are true then the answer is “no”. Skip to question number 4.

- 2. Does request originate from within a physically secure location as described in Section 5.9.1?

If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 3.

- a. The IP address is attributed to a physically secure location; or
- b. If a mnemonic is used it is attributed to a specific device assigned to a specific physically secure location.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

- 3. Are all required technical controls implemented at this location or at the controlling agency?

If either (a) or (b) below are true the answer to the above question is “yes”. Decision tree completed. AA requirement waived.

- a. Appropriate technical controls listed in Sections 5.5 and 5.10 are implemented; or
- b. The controlling agency (i.e. parent agency or agency leveraged as conduit to CJI) extends its wide area network controls down to the requesting agency and the extended controls provide assurance equal or greater to the controls listed in Sections 5.5 and 5.10.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

- 4. Does request originate from an agency-controlled user device?

If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 5.

- a. The static IP address or MAC address can be traced to registered device; or
- b. Certificates are issued to agency managed devices only and certificate exchange is allowed only between authentication server and agency issued devices.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

- 5. Is the agency managed user device associated with and located within a criminal justice conveyance?

If any of the (a), (b), or (c) statements below is true the answer to the above question is “yes”. Proceed to Figure 9 Step 3.

- a. The static IP address or MAC address is associated with a device associated with a criminal justice conveyance; or

- b. The certificate presented is associated with a device associated with a criminal justice conveyance; or
- c. The mnemonic presented is associated with a specific device assigned and that device is attributed to a criminal justice conveyance.

If none of the (a), (b), or (c) statements above are true then the answer is “no”. Skip to question number 7.

6. Is the user device an agency-issued and controlled smartphone or tablet?

If both (a) and (b) below are true, the answer to the above question is “yes.” Proceed to question number 7.

- a. The law enforcement agency issued the device to an individual; and
- b. The device is subject to administrative management control of the issuing agency.

If either (a) or (b) above is false, then the answer is “no.” Decision tree completed. AA required.

7. Does the agency-issued smartphone or tablet have CSO-approved AA compensating controls implemented?

If (a) and (b) below are true, the answer to the above question is “yes.” Decision tree completed. AA requirement is waived.

- a. An agency cannot meet a requirement due to legitimate technical or business constraints; and
- b. The CSO has given written approval permitting AA compensating controls to be implemented in lieu of the required AA control measures.

If either (a) or (b) above is false then the answer is “no.” Decision tree completed. AA required.

5.6.3 Identifier and Authenticator Management

The agency shall establish identifier and authenticator management processes.

5.6.3.1 Identifier Management

In order to manage user identifiers, agencies shall:

- 1. Uniquely identify each user.
- 2. Verify the identity of each user.
- 3. Receive authorization to issue a user identifier from an appropriate agency official.
- 4. Issue the user identifier to the intended party.
- 5. Disable the user identifier after a specified period of inactivity.
- 6. Archive user identifiers.

5.6.3.2 Authenticator Management

In order to manage information system authenticators, agencies shall:

1. Define initial authenticator content.
2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
3. Change default authenticators upon information system installation.
4. Change/refresh authenticators periodically.

Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

5.6.4 Assertions

Identity providers can be leveraged to identify individuals and assert the individual's identity to a service or to a trusted broker who will in-turn assert the identity to a service. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be:

1. Digitally signed by a trusted entity (e.g., the identity provider).
2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.

Assertions generated by a verifier shall expire after 12 hours and shall not be accepted thereafter by the relying party.

Figure 8 – Advanced Authentication Use Cases

Use Case 1 - A Local Police Department Authentication Control Scenario

During the course of an investigation, a detective attempts to access Criminal Justice Information (CJI) from a hotel room using an agency issued mobile broadband card. To gain access, the detective first establishes the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption). Upon connecting to the agency network, the detective is challenged for a username (identification), password ("something you know"), and a one-time password OTP ("something you have") from a hardware token to satisfy the requirement for advanced authentication. Once the detective's credentials are validated, his identity is asserted by the infrastructure to all authorized applications needed to complete his queries.

Use Case 2 – Use of a Smart Card

A user is issued a smart card that is loaded with user-specific digital certificates from a terminal within a controlled area. The user selects an application that will provide access to

Criminal Justice Information (CJI) then enters the proper username (identification) and password (“something you know”). Once prompted, the user connects the smart card (“something you have”) to the terminal. The user is prompted to enter a personal identification number (PIN) to unlock the smart card. Once unlocked, the smart card sends the certificates to the authentication management server at the local agency where the combined username, password, and digital user certificates are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 3 – Out of Band One-Time-Password (OTP) – Mobile phone-based

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password (“something you know”). Once that has been completed, a text message containing a one-time password (OTP) is sent via text message (out of band) to the user’s agency-issued cell phone. The user is challenged via the CJI application for that OTP. The user enters the OTP (“something you have”) then the username, password, and OTP are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 4 – Improper Use of a One-Time-Password (OTP) – Laptop

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password (“something you know”). Once that has been completed, a one-time password (OTP) is sent to the user’s agency-issued laptop (in band) via pop-up message. The user is challenged via the CJI application for that OTP; however, the delivery of the OTP to the device that is being used to access CJI (in band) defeats the purpose of the second factor. This method does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI. See the below explanation:

This method of receiving the necessary OTP (in band) does not guarantee the authenticity of the user’s identity because anyone launching the CJI application and entering a valid username/password combination is presented the OTP via a pop-up which is intend to be the second factor of authentication. This method makes the application accessible to anyone with knowledge of the valid username and password. Potentially, this is no more secure than using only a single factor of authentication.

Use Case 5 – Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires email access (containing Criminal Justice Information) via an Outlook Web Access (OWA) client utilizes a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username

(identification) and a password (“something you know”). The RBA detects this computer has not previously been used by the user, is not listed under the user’s profile, and then presents high-risk challenge/response question(s) which the user is prompted to answer. Once the questions have been verified as correct, the user is authenticated and granted access to the email. Meanwhile, the RBA logs and collects a number of device forensic information and captures the user pattern analysis to update the user’s profile. The CJIS Security Policy requirements for RBA have been satisfied.

Use Case 6 – Improper Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires access to email containing Criminal Justice Information (CJI) via an Outlook Web Access (OWA) client utilizing a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password (“something you know”). The RBA detects this computer has not previously been used by the user and is not listed under the user’s profile. The user is prompted to answer high-risk challenge/response questions for verification and authorization to access to the email; however, if the second authentication factor is to answer additional questions presented every time the user logs on, then this solution is referred to as a knowledge-based authentic on (KBA) solution. A KBA solution does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI.

See the below explanation:

A KBA solution is not a viable advanced authentication (AA) solution per the CJIS Security Policy (CSP). The KBA asks questions and compares the answers to those stored within the user’s profile. A KBA is neither a CSP compliant two factor authentication solution, nor does it meet the CSP criteria of a risk-based authentication (RBA) solution which logs and collects a number of device forensic information and captures the user pattern analysis to update the user’s profile. Using this collected data, the RBA presents challenge/response questions when changes to the user’s profile are noted versus every time the user logs in.

Use Case 7 – Advanced Authentication Compensating Controls on Agency-Issued Smartphones

An authorized user is issued a smartphone that is administratively managed by the agency-installed mobile device management (MDM) solution to ensure device compliance with the CJIS Security Policy. The user initiates an email client on the smartphone that contains emails with CJI. The email client challenges the user to enter a username (identification) and a password (one factor: something you know) which are forwarded to the local agency for authentication. The smartphone lacks the technical capability to challenge the user for a second factor of authentication. This email client is used across the state agency so access is a necessity for the user’s job functions.

An audit by the CSA identifies the agency’s use of the agency smartphone as not compliant with AA requirements due to the authorized user authenticating with only one factor instead of the required two factors.

Subsequently, the agency performs a risk assessment of their smartphone authentication solution and document a legitimate technical constraint due to the lack of technical solutions for smartphone-based two-factor authentication. The risk assessment identifies the following compensating controls that, when combined with the authorized user authenticating to the local agency with their password, meet the intent of the AA requirement by providing a similar level of security:

1. Enhance smartphone policy to enable possession of the smartphone to be considered a factor of authentication (i.e. something you have). Require authorized users to treat the smartphone as a controlled device and protect it as they would a personal credit card or an issued firearm to ensure only they will be in possession of the device
2. Move the email client used to authenticate with the local agency inside an encrypted, password-protected secure container on the smartphone ensuring only the authorized user can access the email application to authenticate.

The agency submits an AA compensating controls request to the CSO outlining the technical constraint identified by the risk assessment, what compensating controls will be employed, and the desired duration of the compensating controls.

The CSO approves the agency's request and provides documentation of the approval to the agency to maintain for audit purposes. The agency enacts the compensating controls and informs agency personnel they are permitted to access CJI via the agency-issued smartphone.

Figure 9 – Authentication Decision for Known Location

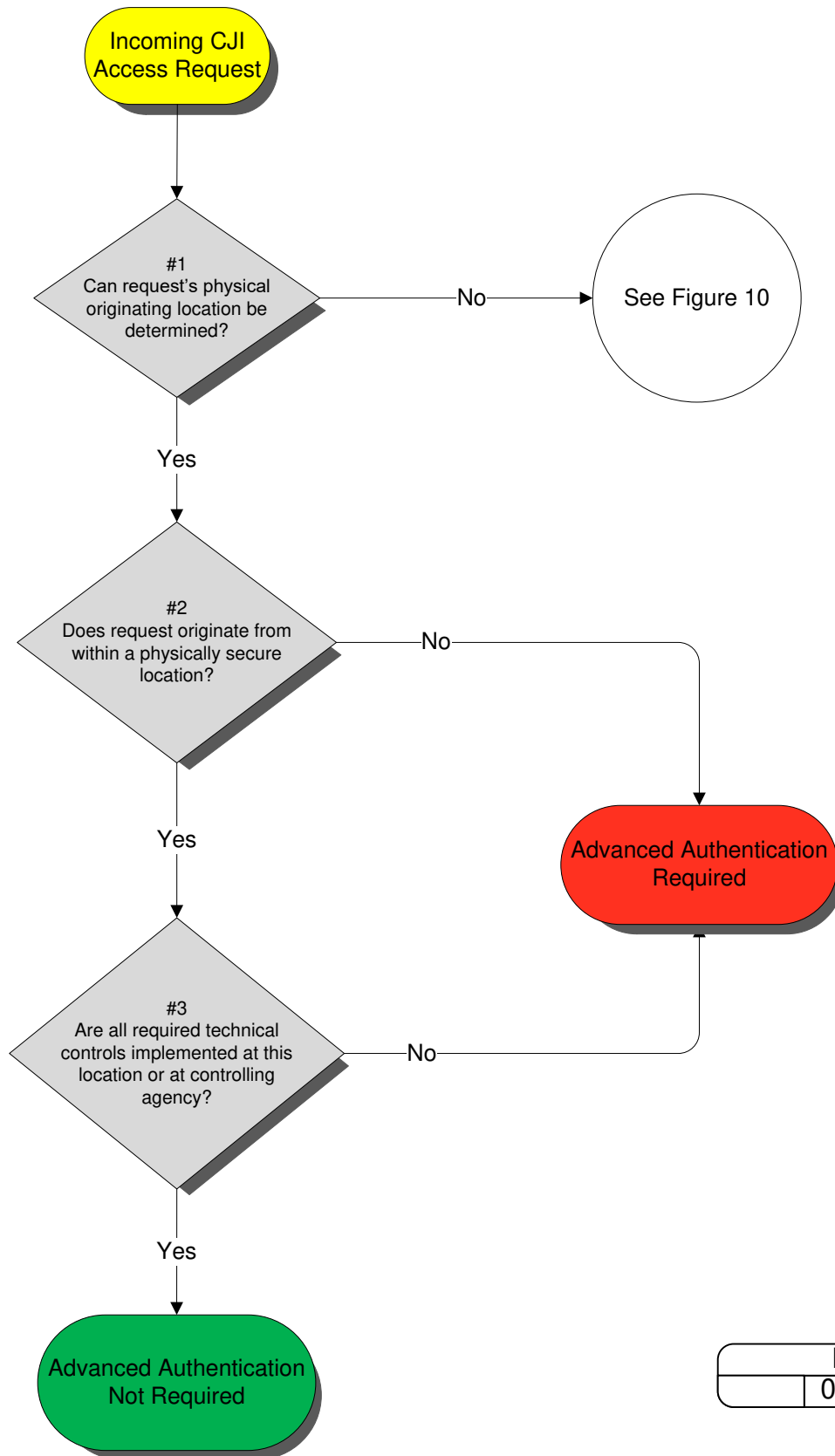


Figure 9		
	08/04/2014	

Figure 10 – Authentication Decision for Unknown Location

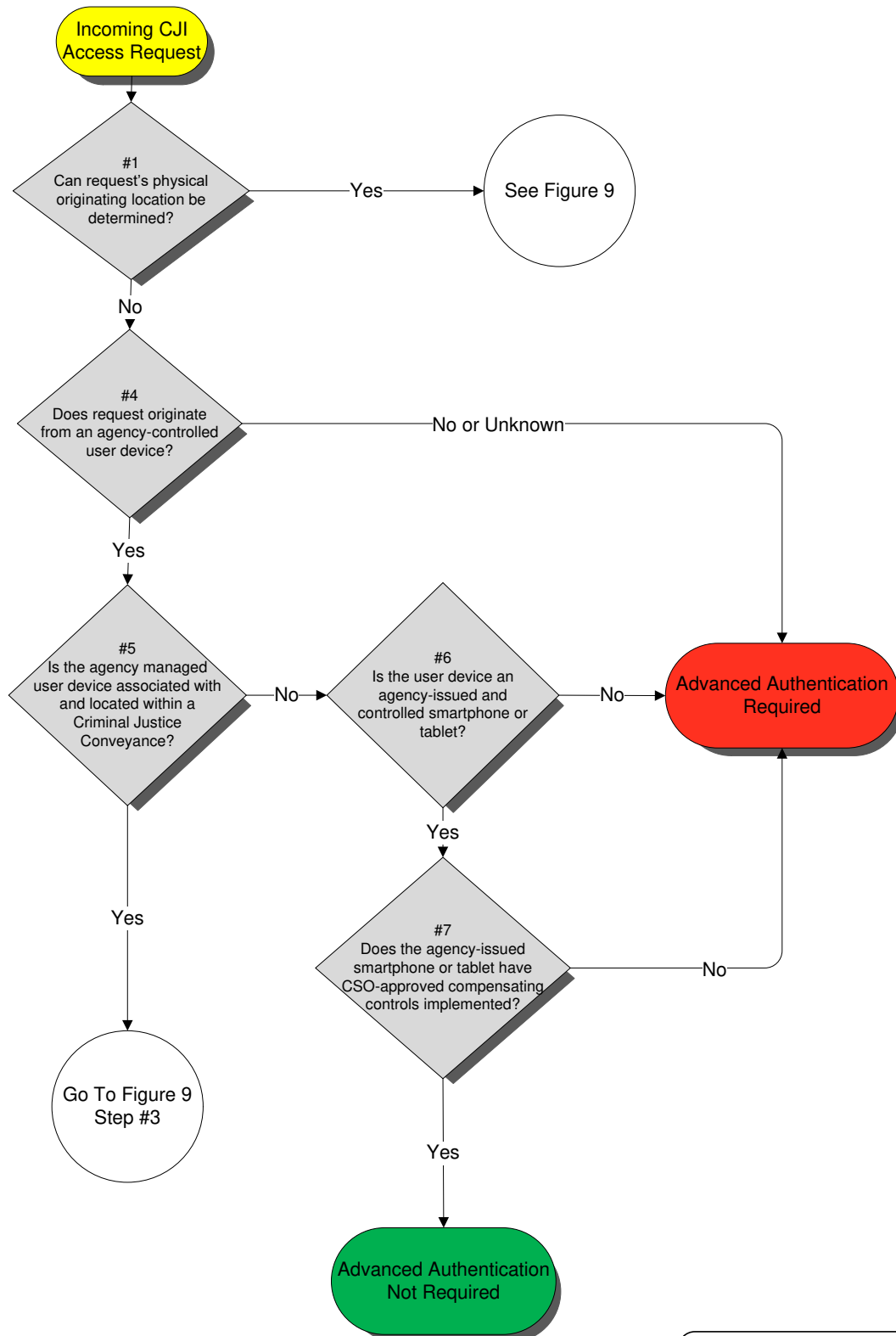


Figure 10		
	10/06/2015	

5.7 Policy Area 7: Configuration Management

5.7.1 Access Restrictions for Changes

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Section 5.5, Access Control, describes agency requirements for control of privileges and restrictions.

5.7.1.1 Least Functionality

The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

5.7.1.2 Network Diagram

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. “For Official Use Only” (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.

5.7.2 Security of Configuration Documentation

The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

Figure 11 – A Local Police Department’s Configuration Management Controls

A local police department decided to update their CAD system, and in doing so tracked all changes made to their infrastructure in a configuration management journal, updated their network topology documents to include all new components in their architecture, then marked all documentation as FOUO and stored them securely.

5.8 Policy Area 8: Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

5.8.1 Media Storage and Access

The agency shall securely store digital and physical media within physically secure locations or controlled areas. The agency shall restrict access to digital and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

5.8.2 Media Transport

The agency shall protect and control digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

5.8.2.1 Digital Media during Transport

Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.

5.8.2.2 Physical Media in Transit

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

5.8.3 Digital Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

Figure 12 – A Local Police Department’s Media Management Policies

A local police department implemented a replacement CAD system that integrated to their state’s CSA and was authorized to process CJI. The police department contracted with an off-site media manager to store backups of their data in the contractor’s vaults, but the contractor was not authorized to process or store CJI. To ensure the confidentiality of the police department’s data while outside its perimeter, they encrypted all data going to the contractor with an encryption product that is FIPS 140-2 certified. The police department rotated and reused media through the contractor’s vaults periodically, and when it required destruction, the police department incinerated the media to irreversibly destroy any data on it.

5.9 Policy Area 9: Physical Protection

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

5.9.1 Physically Secure Location

A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

Sections 5.9.1.1 – 5.9.1.8 describe the physical controls required in order to be considered a physically secure location, while Sections 5.2 and 5.12, respectively, describe the minimum security awareness training and personnel security controls required for unescorted access to a physically secure location. Sections 5.5, 5.6.2.2.1, and 5.10 describe the requirements for technical security controls required to access CJI from within the perimeter of a physically secure location without AA.

5.9.1.1 Security Perimeter

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

5.9.1.2 Physical Access Authorizations

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

5.9.1.3 Physical Access Control

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

5.9.1.4 Access Control for Transmission Medium

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

5.9.1.5 Access Control for Display Medium

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

5.9.1.6 Monitoring Physical Access

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

5.9.1.7 Visitor Control

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

5.9.1.8 Delivery and Removal

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

5.9.2 Controlled Area

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
2. Lock the area, room, or storage container when unattended.
3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
4. Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data “at rest”) of CJI.

Figure 13 – A Local Police Department's Physical Protection Measures

A local police department implemented a replacement CAD system that was authorized to process CJI over an encrypted VPN tunnel to the state's CSA. The police department established a physically separated wing within their precinct separated by locked doors, walls, and a monitored security system within which CJI was processed by criminal justice professionals. Only those persons with the appropriate authorizations were permitted within this wing unless accompanied by such a person. Within this secure wing the police department further segregated the back-office information systems' infrastructure within a separately controlled area restricted only to those authorized administrative personnel with a need to enter.

5.10 Policy Area 10: System and Communications Protection and Information Integrity

Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the policy for protecting systems and communications infrastructures.

Refer to Section 5.13.4 for additional system integrity requirements related to mobile devices used to access CJI.

5.10.1 Information Flow Enforcement

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.
2. Block outside traffic that claims to be from within the agency.
3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

5.10.1.1 Boundary Protection

The agency shall:

1. Control access to networks processing CJI.
2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.3 for guidance on personal firewalls.
4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device "fails closed" vs. "fails open").

6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.

5.10.1.2 Encryption

Encryption is a form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information. Decryption is the reversing of the cryptographic operation to convert the information back into a plaintext (readable) format. There are two main types of encryption: symmetric encryption and asymmetric encryption (also known as public key encryption). Hybrid encryption solutions do exist and use both asymmetric encryption for client/server certificate exchange – session integrity and symmetric encryption for bulk data encryption – data confidentiality.

5.10.1.2.1 Encryption for CJI in Transit

When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.

NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

EXCEPTIONS:

1. See Sections 5.13.1.2.2 and 5.10.2.
2. Encryption shall not be required if the transmission medium meets all of the following requirements:
 - a. The agency owns, operates, manages, or protects the medium.
 - b. Medium terminates within physically secure locations at both ends with no interconnections between.
 - c. Physical access to the medium is controlled by the agency using the requirements in Sections 5.9.1 and 5.12.
 - d. Protection includes safeguards (e.g., acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g., alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.
 - e. With prior approval of the CSO.

Examples:

- A campus is completely owned and controlled by a criminal justice agency (CJA)
 - If line-of-sight between buildings exists where a cable is buried, encryption is not required.

- A multi-story building is completely owned and controlled by a CJA – If floors are physically secure or cable runs through non-secure areas are protected, encryption is not required.
- A multi-story building is occupied by a mix of CJAs and non-CJAs – If floors are physically secure or cable runs through the non-secure areas are protected, encryption is not required.

5.10.1.2.2 Encryption for CJI at Rest

When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

1. When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:
 - a. Be at least 10 characters
 - b. Not be a dictionary word.
 - c. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
 - d. Be changed when previously authorized personnel no longer require access.
2. Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.

NOTE: Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised.

5.10.1.2.3 Public Key Infrastructure (PKI) Technology

For agencies using public key infrastructure (PKI) technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:

1. Include authorization by a supervisor or a responsible official.
2. Be accomplished by a secure process that verifies the identity of the certificate holder.
3. Ensure the certificate is issued to the intended party.

5.10.1.3 Intrusion Detection Tools and Techniques

Intrusion detection systems are deployed inside a network to monitor events against a known set of parameters (i.e. malicious activity or policy violations) and make notification to the system of any event which violates any of those parameters. They are passive in nature, listening and

monitoring network traffic. There are mainly two types of IDS; network-based IDS (NIDS) and host-based IDS (HIDS).

Intrusion prevention systems are an IDS with the capability to respond to detected intrusions. They are normally deployed at the perimeter of a network, scanning traffic. Like detection systems, protection systems compare scanned traffic to defined normal parameters but unlike detection systems are able to take some type of immediate action to mitigate, or prevent, an event.

Agencies shall:

1. Implement network-based and/or host-based intrusion detection or prevention tools.
2. Maintain current intrusion detection or prevention signatures.
3. Monitor inbound and outbound communications for unusual or unauthorized activities.
4. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
5. Review intrusion detection or prevention logs weekly or implement automated event notification.
6. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

5.10.1.4 Voice over Internet Protocol

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are lower costs than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors.

In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:

1. Establish usage restrictions and implementation guidance for VoIP technologies.
2. Change the default administrative password on the IP phones and VoIP switches.
3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.

Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

5.10.1.5 Cloud Computing

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-

145, and 800-146), as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e. U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).

Note: This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (i.e. the Preventing and Combating Serious Crime (PCSC) agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).

Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its “intended use” is detailed within the service agreement. Such authorized uses of metadata may include, but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content – similar to Section 5.4), data usage/indexing metrics, and diagnostic/syslog data.

5.10.2 Facsimile Transmission of CJI

CJI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements. CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in Section 5.10.

5.10.3 Partitioning and Virtualization

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.

5.10.3.1 Partitioning

The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.

The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.

2. Different central processing units.
3. Different instances of the operating system.
4. Different network addresses.
5. Other methods approved by the FBI CJIS ISO.

5.10.3.2 Virtualization

Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines (VMs) that process CJI internally or be separated by a virtual firewall.
4. Drivers that serve critical functions shall be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system – secured as independently as possible.

The following additional technical security controls shall be applied in virtual environments where CJI is comingled with non-CJI:

1. Encrypt CJI when stored in a virtualized environment where CJI is comingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.
2. Encrypt network traffic within the virtual environment.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Implement IDS and/or IPS monitoring within the virtual environment.
2. Virtually or physically firewall each VM within the virtual environment to ensure that only allowed protocols will transact.
3. Segregate the administrative duties for the host.

Appendix G-1 provides some reference and additional background information on virtualization.

5.10.4 System and Information Integrity Policy and Procedures

5.10.4.1 Patch Management

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.
2. Rollback capabilities when installing patches, updates, etc.
3. Automatic updates without individual user intervention.
4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

5.10.4.2 Malicious Code Protection

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

5.10.4.3 Spam and Spyware Protection

The agency shall implement spam and spyware protection.

The agency shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
2. Employ spyware protection at workstations, servers and mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.

5.10.4.4 Security Alerts and Advisories

The agency shall:

1. Receive information system security alerts/advisories on a regular basis.
2. Issue alerts/advisories to appropriate personnel.
3. Document the types of actions to be taken in response to security alerts/advisories.
4. Take appropriate actions in response.

5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

5.10.4.5 Information Input Restrictions

The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.

Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Figure 14 – System and Communications Protection and Information Integrity Use Cases

Use Case 1 – A Local Police Department’s Information Systems & Communications Protections

A local police department implemented a replacement CAD system within a physically secure location that was authorized to process CJI using a FIPS 140-2 encrypted VPN tunnel over the Internet to the state’s CSA. In addition to the policies, physical and personnel controls already in place, the police department employed firewalls both at their border and at key points within their network, intrusion detection systems, a patch-management strategy that included automatic patch updates where possible, virus scanners, spam and spyware detection mechanisms that update signatures automatically, and subscribed to various security alert mailing lists and addressed vulnerabilities raised through the alerts as needed.

Use Case 2 – Faxing from a Single/Multi-function Device over a Traditional Telephone Line

A dispatcher from county A runs a NCIC query on an individual. The results are printed and then sent to an adjoining county using a single/multi-function device with facsimile capability. For faxing, the device is only connected to a traditional telephone line as is the device at the receiving county. Encryption of a document containing CJI is not required because the document travels over a traditional telephone line.

Use Case 3 – Faxing from a Multi-function Device over a Network

A dispatcher from city A runs a NCIC query on an individual. The results are printed and the dispatcher uses a multi-function copier to fax the file to a city in another state. The dispatcher enters the fax number of the receiver and sends the document. The document containing CJI is automatically converted to a digital file and routed to the receiver over the agency network and the Internet. Because the device uses a network and the Internet for transmitting documents containing CJI, encryption in transit using FIPS 140-2 certified 128 bit symmetric encryption is required.

5.11 Policy Area 11: Formal Audits

Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.

5.11.1 Audits by the FBI CJIS Division

5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

5.11.1.2 Triennial Security Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.

5.11.2 Audits by the CSA

Each CSA shall:

1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.
3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
4. Have the authority, on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.

Note: This authority does not apply to the audit requirement outlined in the Security and Management Control Outsourcing Standard for Non-Channeler and Channelers related to outsourcing noncriminal justice administrative functions.

5.11.3 Special Security Inquiries and Audits

All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.

5.11.4 Compliance Subcommittees

The Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) established the Compliance Evaluation Subcommittee (CES) to evaluate the results of audits conducted by the CJIS Audit Unit (CAU). The CES makes specific recommendations to the APB concerning compliance with applicable policies and regulations. The most current information regarding the CAU audits that are within the purview of the CES and detailed CES sanctions process procedures are available at CJIS.gov (Law Enforcement Enterprise Portal) CJIS Special Interest Groups CES Section and CJIS Section of FBI.gov.

The National Crime Prevention and Privacy Compact (Compact) Council at Article VI established the Compact Council (Council). The Compact Council Sanctions Committee is responsible for ensuring the use of the Interstate Identification Index System for noncriminal justice purposes complies with the Compact and with rules, standards, and procedures established by the Compact Council. As such, the Sanctions Committee reviews the results of audits conducted by the Federal Bureau of Investigation (FBI) of participants in the FBI's Criminal Justice Services (CJIS) Division programs. The Sanctions Committee reviews the audit results and the participant's response to determine a course of action necessary to bring the participant into compliance and make recommendations to the Compact Council or the FBI. Additional information on the Compact Council Sanctions process is available on the Compact Council's web-site.

Figure 15 – The Audit of a Local Police Department

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. Shortly after the implementation, their state's CSA conducted an audit of their policies, procedures, and systems that process CJI. The police department supplied all architectural and policy documentation, including detailed network diagrams, to the auditors in order to assist them in the evaluation. The auditors discovered a deficiency in the police department's systems and marked them "out" in this aspect of the FBI CJIS Security Policy. The police department quickly addressed the deficiency and took corrective action, notifying the auditors of their actions.

5.12 Policy Area 12: Personnel Security

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have unescorted access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI

1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing). However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:
 - a. 5 CFR 731.106; and/or
 - b. Office of Personnel Management policy, regulations, and guidance; and/or
 - c. agency policy, regulations, and guidance.

Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.
3. If a record of any kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.
 - a. If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI. However, the Interface Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
 - b. Applicants with a record of misdemeanor offense(s) may be granted access if the CSO, or his or her designee, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The Interface Agency may request the CSO review a denial of access determination. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.
 - c. If a record of any kind is found on a contractor, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the contractor's security officer.

4. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.
6. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
7. The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

5.12.2 Personnel Termination

Upon termination of personnel by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI. Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems is terminated. If the employee is an employee of a NCJA or a Contractor, the employer shall notify all Interface Agencies that may be affected by the personnel change.

5.12.3 Personnel Transfer

The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.

5.12.4 Personnel Sanctions

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Figure 16 – A Local Police Department's Personnel Security Controls

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. In addition to the physical and technical controls already in place, the police department implemented a variety of personnel security controls to reduce the insider threat. The police department used background screening consistent with the FBI CJIS Security Policy to vet those with unescorted access to areas in which CJI is processed, including the IT administrators employed by a contractor and all janitorial staff. The police department established sanctions against any vetted person found to be in violation of stated

policies. The police department re-evaluated each person's suitability for access to CJI every five years.

5.13 Policy Area 13: Mobile Devices

This policy area describes considerations and requirements for mobile devices including smartphones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices.

The agency shall: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

Appendix G provides reference material and additional information on mobile devices.

5.13.1 Wireless Communications Technologies

Examples of wireless communication technologies include, but are not limited to: 802.11, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described below.

5.13.1.1 802.11 Wireless Protocols

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.

Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
5. Enable user authentication and encryption mechanisms for the management interface of the AP.
6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Section 5.6.2.1.
7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.

8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
11. Ensure that the ad hoc mode has been disabled.
12. Disable all nonessential management protocols on the APs.
13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.
14. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

5.13.1.2 Cellular Devices

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), tablets, personal digital assistants (PDA), and “aircards” are examples of cellular handheld devices or devices that are capable of employing cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of the criminal justice professional).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

5.13.1.2.1 Cellular Service Abroad

Certain internal functions on cellular devices may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider which is considered a “trusted” entity by the device.

When devices are authorized to access CJI outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency’s policies prior to and after deployment outside of the U.S.

5.13.1.2.2 Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements.

5.13.1.3 Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth is used primarily to establish wireless personal area networks (WPAN). Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices.

Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g. denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency’s operational and business processes.

5.13.1.4 Mobile Hotspots

Many mobile devices include the capability to function as a WiFi hotspot that allows other devices to connect through the device to the internet over the devices cellular network.

When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured:

1. Enable encryption on the hotspot
2. Change the hotspot’s default SSID
 - a. Ensure the hotspot SSID does not identify the device make/model or agency ownership
3. Create a wireless network password (Pre-shared key)
4. Enable the hotspot’s port filtering/blocking features if present
5. Only allow connections from agency controlled devices

Note: Refer to the requirements in Section 5.10.1.2 encryption for item #1. Refer to the requirements in Section 5.6.2.2.1 Password for item #3. Only password attributes #1, #2 and #3 are required.

OR

1. Have a MDM solution to provide the same security as identified in items 1 – 5 above.

5.13.2 Mobile Device Management (MDM)

Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency.

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of full featured operating systems may not function properly on devices with limited feature operating systems. MDM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time. Agencies shall implement the following controls when allowing CJI access from devices running a limited-feature operating system:

1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration configured and implemented to perform at least the following controls:
 - a. Remote locking of device
 - b. Remote wiping of device
 - c. Setting and locking device configuration
 - d. Detection of “rooted” and “jailbroken” devices
 - e. Enforcement of folder or disk level encryption
 - f. Application of mandatory policy settings on the device
 - g. Detection of unauthorized configurations
 - h. Detection of unauthorized software or applications
 - i. Ability to determine the location of agency controlled devices
 - j. Prevention of unpatched devices from accessing CJI or CJI systems
 - k. Automatic device wiping after a specified number of failed access attempts

EXCEPTION: An MDM is not required when receiving CJI from an indirect access information system (i.e. the system provides no capability to conduct transactional activities on state and national repositories, applications or services). However, it is incumbent upon the authorized agency to ensure CJI is delivered to the appropriate requesting agency or individual. The CSO will make the final determination of whether access is considered indirect.

5.13.3 Wireless Device Risk Mitigations

Organizations shall, at a minimum, ensure that wireless devices:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.

2. Are configured for local device authentication (see Section 5.13.7.1).
3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.
4. Encrypt all CJI resident on the device.
5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.
6. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.

5.13.4 System Integrity

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full featured operating systems. In many cases, the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM, application, or supporting service infrastructure.

5.13.4.1 Patching/Updates

Based on the varying connection methods for mobile devices, an always on connection cannot be guaranteed for patching and updating. Devices without always-on cellular connections may not be reachable for extended periods of time by the MDM or solution either to report status or initiate patching.

Agencies shall monitor mobile devices to ensure their patch and update state is current.

5.13.4.2 Malicious Code Protection

Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software and can provide a high degree of confidence that only known software or applications are installed on the device.

Agencies that allow smartphones and tablets to access CJI shall have a process to approve the use of specific software or applications on the devices. Any device natively capable of performing these functions without a MDM solution is acceptable under this section.

5.13.4.3 Personal Firewall

For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.

2. Block unsolicited requests to connect to the user device.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

Mobile devices with limited feature operating systems (i.e. tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform functions similar to a personal firewall on a device with a full feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

5.13.5 Incident Response

In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control. For example:
 - a. Device known to be locked, minimal duration of loss
 - b. Device lock state unknown, minimal duration of loss
 - c. Device lock state unknown, extended duration of loss
 - d. Device known to be unlocked, more than momentary duration of loss
2. Total loss of device
3. Device compromise
4. Device loss or compromise outside the United States

5.13.6 Access Control

Multiple user accounts are not generally supported on limited feature mobile operating systems. Access control (Section 5.5 Access Control) shall be accomplished by the application that accesses CJI.

5.13.7 Identification and Authentication

Due to the technical methods used for identification and authentication on many limited feature mobile operating systems, achieving compliance may require many different components.

5.13.7.1 Local Device Authentication

When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use. The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators.

5.13.7.2 Advanced Authentication

When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user unless the access to CJI is indirect as described in Section 5.6.2.2.1. If access is indirect, then AA is not required.

5.13.7.2.1 Compensating Controls

CSO approved compensating controls to meet the AA requirement on agency-issued smartphones and tablets with limited feature operating systems are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required AA control measures when an agency cannot meet a requirement due to legitimate technical or business constraints. Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.13.2. The compensating controls shall:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls
4. Expire upon the CSO approved date or when a compliant AA solution is implemented.

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

The compensating controls for AA are a combination of controls providing acceptable assurance only the authorized user is authenticating and not an impersonator or (in the case of agency-issued device used by multiple users) controls that reduce the risk of exposure if information is accessed by an unauthorized party.

The following minimum controls shall be implemented as part of the CSO approved compensating controls:

- Possession and registration of an agency issued smartphone or tablet as an indication it is the authorized user
- Use of device certificates per Section 5.13.7.3 Device Certificates
- Implemented CJIS Security Policy compliant standard authenticator protection on the secure location where CJI is stored

5.13.7.3 Device Certificates

Device certificates are often used to uniquely identify mobile devices using part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of device identification or authentication in a larger scheme, a device certificate alone placed on the device shall not be considered valid proof that the device is being operated by an authorized user.

When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be:

1. Protected against being extracted from the device
2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts
3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use

APPENDICES

APPENDIX A TERMS AND DEFINITIONS

Access to Criminal Justice Information — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Administration of Criminal Justice — The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes “crime prevention programs” to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or “safe house” programs) and the result of such checks will not be disseminated outside the law enforcement agency.

Agency Controlled Mobile Device — A mobile device that is centrally managed by an agency for the purpose of securing the device for potential access to CJI. The device can be agency issued or BYOD (personally owned).

Agency Coordinator (AC) — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.

Agency Issued Mobile Device — A mobile device that is owned by an agency and issued to an individual for use. It is centrally managed by the agency for the purpose of securing the device for potential access to CJI. The device is not BYOD (personally owned).

Agency Liaison (AL) — Coordinator of activities between the criminal justice agency and the noncriminal justice agency when responsibility for a criminal justice system has been delegated by a criminal justice agency to a noncriminal justice agency, which has in turn entered into an agreement with a contractor. The agency liaison shall, inter alia, monitor compliance with system security requirements. In instances in which the noncriminal justice agency's authority is directly from the CJIS systems agency, there is no requirement for the appointment of an agency liaison.

Asymmetric Encryption — A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Authorized Recipient — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Availability — The degree to which information, a system, subsystem, or equipment is operable and in a useable state; frequently represented as a proportion of time the element is in a functioning condition.

Biographic Data — Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

Biometric Data — When applied to CJI, it is used to identify individuals, and includes the following types: fingerprints, palm prints, DNA, iris, and facial recognition.

Case / Incident History — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regards to CJI, it is the information about the history of criminal incidents.

Certificate Authority (CA) Certificate – Digital certificates required for certificate-based authentication that are issued to tell the client computers and servers that it can trust other certificates that are issued by this CA.

Channeler — A FBI approved contractor, who has entered into an agreement with an Authorized Recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The Channeler ensures fingerprint submissions are properly and adequately completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to Authorized Recipients. A Channeler is essentially an "expediter" rather than a user of criminal history record check results.

Cloud Client – A machine or software application that accesses cloud services over a network connection, perhaps on behalf of a subscriber.

Cloud Computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.

Cloud Provider – An organization that provides cloud computing services.

Cloud Subscriber – A person or organization that is a customer of a cloud computing service provider.

CJIS Advisory Policy Board (APB) — The governing organization within the FBI CJIS Advisory Process composed of representatives from criminal justice and national security agencies within the United States. The APB reviews policy, technical, and operational issues relative to CJIS Division programs and makes subsequent recommendations to the Director of the FBI.

CJIS Audit Unit (CAU) — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the CJIS Security Policy.

CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI CJIS ISO; the document containing this glossary.

CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS

Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

CJIS Systems Agency Information Security Officer (CSA ISO) — The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

CJIS Systems Officer (CSO) — The individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf of the CJIS Systems Agency.

Compact Council — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

Compact Officers — The leadership of the Compact Council, oversees the infrastructure established by the National Crime Prevention and Privacy Compact Act of 1998, which is used by ratifying states to exchange criminal records for noncriminal justice purposes. Their primary responsibilities are to promulgate rules and procedures for the effective and appropriate use of the III system.

Compensating Controls — Compensating controls are temporary control measures implemented in lieu of the required control measures when an agency cannot meet the AA requirement due to legitimate technical or business constraints. The compensating controls must:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

Computer Security Incident Response Capability (CSIRC) — A collection of personnel, systems, and processes that are used to efficiently and quickly manage a centralized response to any sort of computer security incident which may occur.

Confidentiality — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Contractor — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

Contracting Government Agency (CGA) — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

Crime Reports Data — The data collected through the Uniform Crime Reporting program and reported upon annually by the FBI CJIS division used to analyze the crime statistics for the United States.

Criminal History Record Information (CHRI) — A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Agency (CJA) — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Agency User Agreement — A terms-of-service agreement that must be signed prior to accessing CJI. This agreement is required by each CJA and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.

Criminal Justice Conveyance — A criminal justice conveyance is any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods, with the requirements of Section 5.9.1.3.

Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Data — See Information and CJI.

Decryption – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Degauss — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g. solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

Department of Justice (DoJ) — The Department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.

Digital Media – Any form of electronic media designed to store data in a digital format. This includes, but is not limited to: memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Digital Signature – A digital signature consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm that, given a message and a private key, produces a signature. (3) A signature verifying algorithm that, given a message, public key, and a signature, either accepts or rejects the message's claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

Direct Access — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Dissemination — The transmission/distribution of CJI to Authorized Recipients within an agency.

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Escort – Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Facsimile (Fax) – Facsimile is: (a) a document received and printed on a single or multi-function stand-alone device, (b) a single or multi-function stand-alone device for the express purpose of transmitting and receiving documents from a like device over a standard telephone line, or (c) a facsimile server, application, service which implements email-like technology and transfers documents over a network.

Federal Bureau of Investigation (FBI) — The agency within the DOJ responsible to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

FBI CJIS Information Security Officer (FBI CJIS ISO) — The FBI personnel responsible for the maintenance and dissemination of the FBI CJIS Security Policy; the liaison between the FBI and the CSA's ISOs and other relevant security points-of-contact (POCs); the provider of technical guidance as to the intent and implementation of technical policy issues; the POC for computer incident notification which also disseminates security alerts to the CSOs and ISOs.

Federal Information Security Management Act (FISMA) — The Federal Information Security Management Act of 2002, a US Federal law that established information security standards for the protection of economic and national security interests of the United States. It requires each federal agency to develop, document, and implement an agency-wide program to provide information

security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

For Official Use Only (FOUO) — A caveat applied to unclassified sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), 5 U.S.C 522. In general, information marked FOUO shall not be disclosed to anybody except Government (Federal, State, tribal, or local) employees or contractors with a need to know.

Full-feature Operating System — Full-feature operating systems are traditional operating systems used by a standard desktop computer (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). These operating systems are generally open to user control and configuration and therefore require configuration management to properly secure, or “harden”, these devices from malicious network based technical attacks (e.g. malware, spyware, hackers, etc.). These operating systems require traditional protection applications such as antivirus programs and personal firewalls.

Guest Operating System — An operating system that has emulated hardware presented to it by a host operating system. Also referred to as the virtual machine (VM).

Hash Value — The term that refers to an alphanumeric value which represents the result of applying a cryptographic hash function to data.

Hashing — The process of applying a mathematical algorithm to data to produce an alphanumeric value (i.e. hash value) to be used as a representative of that data.

Host Operating System — In the context of virtualization, the operating system that interfaces with the actual physical hardware and arbitrates between it and the guest operating systems. It is also referred to as a hypervisor.

Hybrid Encryption — A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Hypervisor — See Host Operating System.

Identity History Data — Textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.

In-Band – The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is the same as the one used for login.

Indirect Access – Having the authority to access systems containing CJI without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g. CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

Information — See data and CJI.

Information Exchange Agreement — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party’s information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which

establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance.

Information Security Officer (ISO) — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training and awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

Information System — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

Integrated Automated Fingerprint Identification System (IAFIS) — The national fingerprint and criminal history system maintained by the FBI CJIS Division that provides the law enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

Integrity — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.

Interconnection Security Agreement (ISA) — An agreement much like an Information Exchange Agreement as mentioned above, but concentrating more on formalizing the technical and security requirements pertaining to some sort of interface between the parties' information systems.

Interface Agency — A legacy term used to describe agencies with direct connections to the CSA. This term is now used predominantly in a common way to describe any sub-agency of a CSA or SIB that leverages the CSA or SIB as a conduit to FBI CJIS information.

Internet Protocol (IP) — A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Interstate Identification Index (III) — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

Intrusion Detection — The process of monitoring the events occurring in an information system or network and analyzing them for signs of possible incidents.

Intrusion Detection System — Software which automates the intrusion detection process.

Intrusion Prevention — The process of monitoring events occurring in an information system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Intrusion Prevention System — Software which has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Jailbreak (Jailbroken) — The process of attaining privileged control (known as “root access”) of a device running the Apple iOS operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Laptop Devices – Laptop devices are mobile devices with a full-featured operating system (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). Laptops are typically intended for transport via vehicle mount or portfolio-sized carry case, but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones), or mobile devices that feature a limited feature operating system (e.g. tablets).

Law Enforcement Enterprise Portal (LEEP) — A secure, Internet-based communications portal provided by the FBI CJIS Division for use by law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. Its primary purpose is to provide a platform on which various law enforcement agencies can collaborate on FOUO matters.

Limited-feature Operating System — Limited-feature operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers (e.g. Apple iOS, Android, Windows Mobile, Blackberry OS, etc.). These operating systems permit limited user control, but are inherently more resistant than a full-feature operating system to certain types of network based technical attacks due to the limited feature sets. Devices using these operating systems are required to be managed by a mobile device management solution.

Logical Access – The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

Logical Partitioning – When the host operating system, or hypervisor, allows multiple guest operating systems to share the same physical resources.

Local Agency Security Officer (LASO) — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

Management Control Agreement (MCA) — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA’s authority remains with regard to all aspects of Section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.

Metadata — Structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is commonly referred to as data about data, information about information, or information describing the characteristics of data.

Mobile Device — Any portable device used to access CJI via a wireless connection (e.g. cellular, WiFi, Bluetooth, etc.).

Mobile Device Management (MDM) — Centralized administration and control of mobile devices specifically including, but not limited to, cellular phones, smart phones, and tablets. Management typically includes the ability to configure device settings and prevent a user from changing them, remotely locating a device in the event of theft or loss, and remotely locking or wiping a device. Management can also include over-the-air distribution of applications and updating installed applications.

Mobile (WiFi) Hotspot — A mobile (WiFi) hotspot is a zone or area associated with a mobile device (e.g. smartphone, air card) allowing wireless connectivity to the Internet typically through a cellular connection.

National Crime Information Center (NCIC) — An information system which stores CJJ which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

National Instant Criminal Background Check System (NICS) — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

National Institute of Standards and Technology (NIST) — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.

Noncriminal Justice Agency (NCJA) — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

NCJA (Government) — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJJ. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.

NCJA (Private) — A private agency or subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJJ. An example would include a local bank.

NCJA (Public) — A public agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJJ. An example would include a county school board which uses CHRI to assist in employee hiring decisions.

Noncriminal Justice Purpose — The uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Office of Management and Budget (OMB) — The agency within the Executive Branch of the Federal government responsible to oversee the preparation of the federal budget, to assist in the

supervision of other Executive Branch agencies, and to oversee and coordinate the Presidential Administration's procurement, financial management, information, and regulatory policies.

One-time Password — A disposable, single-use standard authenticator for access CJI. One-time passwords are: minimum of six (6) randomly generated characters, valid for a single session, and if not used, expire within a minimum of five (5) minutes after issuance.

Out-of-Band — The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is separate from that used for login.

Outsourcing — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

Outsourcing Standard — National Crime Prevention and Privacy Compact Council's Outsourcing Standard. The Compact Council's uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes.

Partitioning – Managing guest operating system, or virtual machine, access to hardware so that each guest OS can access its own resources but cannot encroach on the other guest operating systems resources or any resources not allocated for virtualization use.

Password Verifier (Verifier) – An entity or process that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.

Personal Firewall — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

Personally Identifiable Information (PII) — PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Physical Access – The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Physical Media – Physical media refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.

Physical Partitioning – When the host operating system, or hypervisor, assigns separate physical resources to each guest operating systems, or virtual machine.

Physically Secure Location — A facility, a criminal justice conveyance, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

Pocket/Handheld Mobile Device – Pocket/Handheld mobile devices (e.g. smartphones) are intended to be carried in a pocket or holster attached to the body and feature an operating system

with limited functionality (e.g., iOS, Android, BlackBerry, etc.). This definition does not include tablet and laptop devices.

Property Data — Information about vehicles and property associated with a crime.

Rap Back — A NGI service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.

Receive-Only Terminal (ROT) – A device that is configured to accept a limited type of data but is technically prohibited from forming or transmitting data, browsing or navigating internal or external networks, or otherwise performing outside the scope of receive only (e.g., a printer, dumb terminal, etc.).

Repository Manager, or Chief Administrator — The designated manager of the agency having oversight responsibility for a CSA’s fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the repository manager and CSO may be the same person.

Root (Rooting, Rooted) — The process of attaining privileged control (known as “root access”) of a device running the Android operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Salting –The process of applying a non-secret value to data prior to applying a cryptographic process, such as hashing. This process changes the value to be hashed in a manner designed to ensure an attacker cannot reuse the results of computations for one instance.

Secondary Dissemination — The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

Security Addendum (SA) — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Sensitive But Unclassified (SBU) — Designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of SBU information have authority in statute or regulation (e.g. SSI, CII) while others, including FOUO, do not. As of May 9, 2008, the more appropriate terminology to use is Controlled Unclassified Information (CUI).

Server/Client Computer Certificate (device-based) – Digital certificates that are issued to servers or client computers or devices by a CA and used to prove device identity between server and/or client computer devices during the authentication process.

Service — The organized system of apparatus, appliances, personnel, etc, that supply some tangible benefit to the consumers of this service. In the context of CJI, this usually refers to one of the applications that can be used to process CJI.

Shredder — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

Smartphone – See pocket/handheld mobile devices.

Social Engineering — The act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

Software Patch — A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems. As such, patches should be installed in a test environment prior to being installed in a live, operational system. Patches often can be found in multiple locations but should be retrieved only from sources agreed upon through organizational policy.

State and Federal Agency User Agreement — A written agreement that each CSA or SIB Chief shall execute with the FBI CJIS Division stating their willingness to demonstrate conformance with the FBI CJIS Security Policy prior to the establishment of connectivity between organizations. This agreement includes the standards and sanctions governing use of CJIS systems, as well as verbiage to allow the FBI to periodically audit the CSA as well as to allow the FBI to penetration test its own network from the CSA's interfaces to it.

State Compact Officer — The representative of a state that is party to the National Crime Prevention and Privacy Compact, and is the chief administrator of the state's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

State Identification Bureau (SIB) — The state agency with the responsibility for the state's fingerprint identification services.

State Identification Bureau (SIB) Chief — The SIB Chief is the designated manager of state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

State of Residency – A state of residency is the state in which an individual claims and can provide documented evidence as proof of being his/her permanent living domicile. CJIS Systems Officers have the latitude to determine what documentation constitutes acceptable proof of residency.

Symmetric Encryption — A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

System — Refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections. In the context of CJI, this usually refers to

applications and all interconnecting infrastructure required to use those applications that process CJI.

Tablet Devices – Tablet devices are mobile devices with a limited feature operating system (e.g. iOS, Android, Windows RT, etc.). Tablets typically consist of a touch screen without a permanently attached keyboard intended for transport via vehicle mount or portfolio-sized carry case but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones) or mobile devices with full-featured operating systems (e.g. laptops).

Terminal Agency Coordinator (TAC) — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

User Certificate (user-based) – Digital certificates that are unique and issued to individuals by a CA. Though not always required to do so, these specific certificates are often embedded on smart cards or other external devices as a means of distribution to specified users. This certificate is used when individuals need to prove their identity during the authentication process.

Virtual Escort – Authorized personnel who actively monitor a remote maintenance session on Criminal Justice Information (CJI)-processing systems. The escort must have the ability to end the session at any time deemed necessary to ensure the protection and integrity of CJI at all times.

Virtual Machine (VM) – See Guest Operating System

Virtualization — Refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation or emulation allowing multiple operating systems, or images, to run concurrently on the same hardware.

Voice over Internet Protocol (VoIP) — A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Wireless Access Point – A wireless access point is a device that logically connects a wireless client device to an organization's enterprise network which processes unencrypted CJI.

Wireless (WiFi) Hotspot – A wireless (WiFi) hotspot is a zone or area within a fixed location allowing wireless connectivity to the Internet typically through a wired connection. Hotspots are typically available in public areas such as airports, hotels and restaurants.

APPENDIX B ACRONYMS

Acronym	Term
AA	Advanced Authentication
AC	Agency Coordinator
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
APB	Advisory Policy Board
BD-ADDR	Bluetooth-Enabled Wireless Devices and Addresses
BYOD	Bring Your Own Device
CAD	Computer-Assisted Dispatch
CAU	CJIS Audit Unit
CFR	Code of Federal Regulations
CGA	Contracting Government Agency
CHRI	Criminal History Record Information
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
ConOps	Concept of Operations
CSA	CJIS Systems Agency
CSIRC	Computer Security Incident Response Capability
CSO	CJIS Systems Officer
DAA	Designated Approving Authority
DoJ	Department of Justice

DoJCERT	DoJ Computer Emergency Response Team
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HTTP	Hypertext Transfer Protocol
IAFIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
III	Interstate Identification Index
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
LASO	Local Agency Security Officer
LEEP	Law Enforcement Enterprise Portal
LMR	Land Mobile Radio
MAC	Media Access Control
MCA	Management Control Agreement
MDM	Mobile Device Management
MITM	Man-in-the-Middle

MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NCJA	Noncriminal Justice Agency
NICS	National Instant Criminal Background Check System
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
OTP	One-time Password
PBX	Private Branch Exchange
PCSC	Preventing and Combating Serious Crime
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point-of-Contact
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QoS	Quality of Service
RCMP	Royal Canadian Mounted Police
RF	Radio Frequency
SA	Security Addendum
SCO	State Compact Officer
SIB	State Identification Bureau

SIG	Special Interest Group
SP	Special Publication
SPRC	Security Policy Resource Center
SSID	Service Set Identifier
TAC	Terminal Agency Coordinator
TLS	Transport Layer Security
UCN	Universal Control Number
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

APPENDIX C NETWORK TOPOLOGY DIAGRAMS

Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the “big picture” – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.

The following diagrams, labeled Appendix C.1-A through C.1-D, are examples for agencies to utilize during the development, maintenance, and update stages of their own network diagrams. By using these example drawings as a guideline, agencies can form the foundation for ensuring compliance with Section 5.7.1.2 of the CJIS Security Policy.

The purpose for including the following diagrams in this Policy is to aid agencies in their understanding of diagram expectations and should not be construed as a mandated method for network topologies. It should also be noted that agencies are not required to use the identical icons depicted in the example diagrams and should not construe any depiction of a particular vendor product as an endorsement of that product by the FBI CJIS Division.

Appendix C.1-A is a conceptual overview of the various types of agencies that can be involved in handling of CJJ, and illustrates several ways in which these interconnections might occur. This diagram is not intended to demonstrate the level of detail required for any given agency’s documentation, but it provides the reader with some additional context through which to digest the following diagrams. Take particular note of the types of network interfaces in use between agencies, in some cases dedicated circuits with encryption mechanisms, and in other cases VPNs over the Internet. This diagram attempts to show the level of diversity possible within the law enforcement community. These diagrams in no way constitute a standard for network engineering, but rather, for the expected quality of documentation.

The next three topology diagrams, C.1-B through C.1-D, depict conceptual agencies. For C.1-B through C.1-D, the details identifying specific “moving parts” in the diagrams by manufacturer and model are omitted, but it is expected that any agencies producing such documentation will provide diagrams with full manufacturer and model detail for each element of the diagram. Note that the quantities of clients should be documented in order to assist the auditor in understanding the scale of assets and information being protected.

Appendix C.1-B depicts a conceptual state law enforcement agency’s network topology and demonstrates a number of common technologies that are in use throughout the law enforcement community (some of which are compulsory per CJIS policy, and some of which are optional) including Mobile Broadband cards, VPNs, Firewalls, Intrusion Detection Devices, VLANs, and so forth. Note that although most state agencies will likely have highly-available configurations, the example diagram shown omits these complexities and only shows the “major moving parts” for clarity but please note the Policy requires the logical location of all components be shown. The level of detail depicted should provide the reader with a pattern to model future documentation from, but should not be taken as network engineering guidance.

Appendix C.1-C depicts a conceptual county law enforcement agency. A number of common technologies are presented merely to reflect the diversity in the community, including proprietary

Packet-over-RF infrastructures and advanced authentication techniques, and to demonstrate the fact that agencies can act as proxies for other agencies.

Appendix C.1-D depicts a conceptual municipal law enforcement agency, presumably a small one that lacks any precinct-to-patrol data communications. This represents one of the smallest designs that could be assembled that, assuming all other details are properly considered, would meet the criteria for Section 5.7.1.2. This diagram helps to demonstrate the diversity in size that agencies handling criminal justice data exhibit.

Figure C-1-A Overview: Conceptual Connections Between Various Agencies

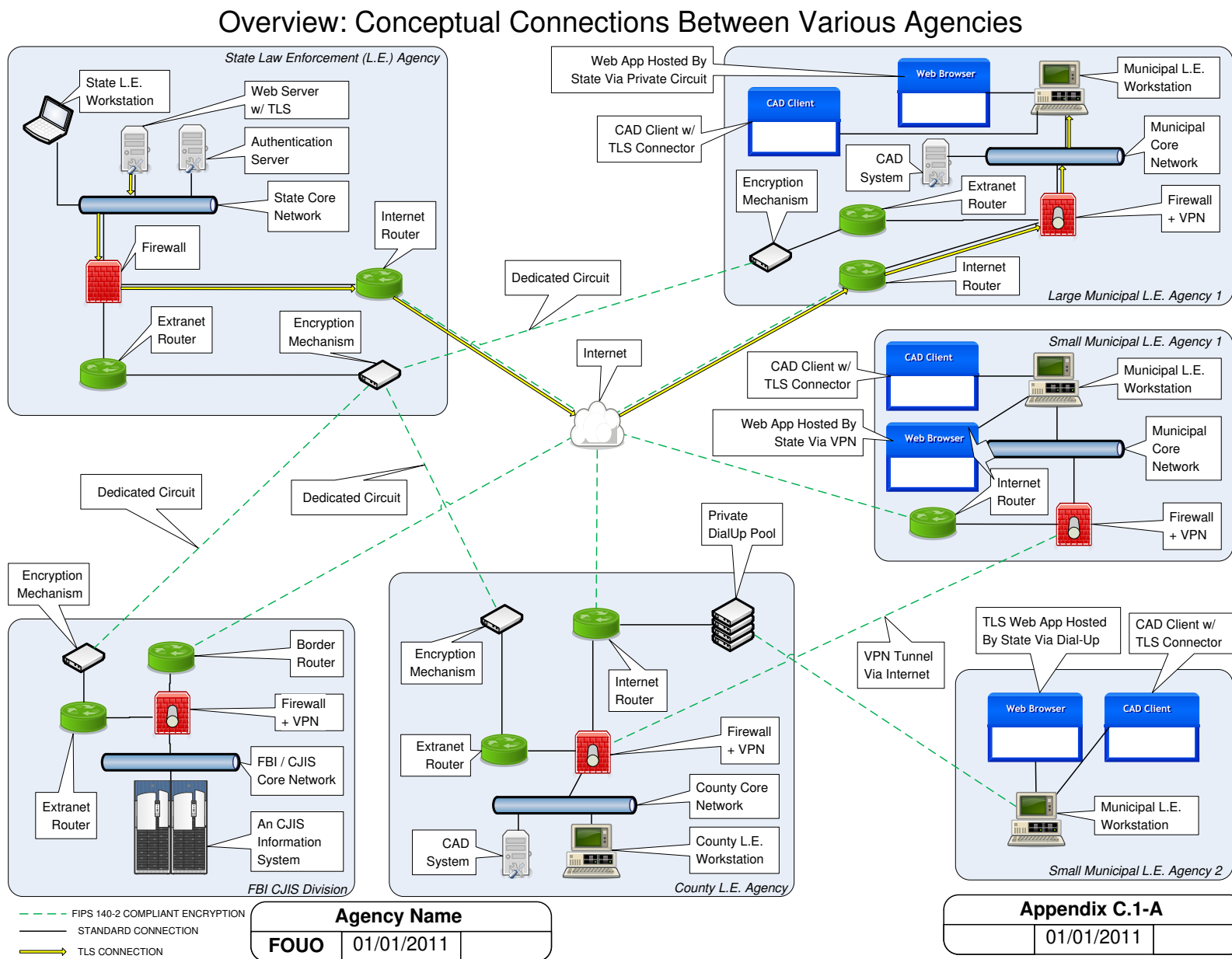
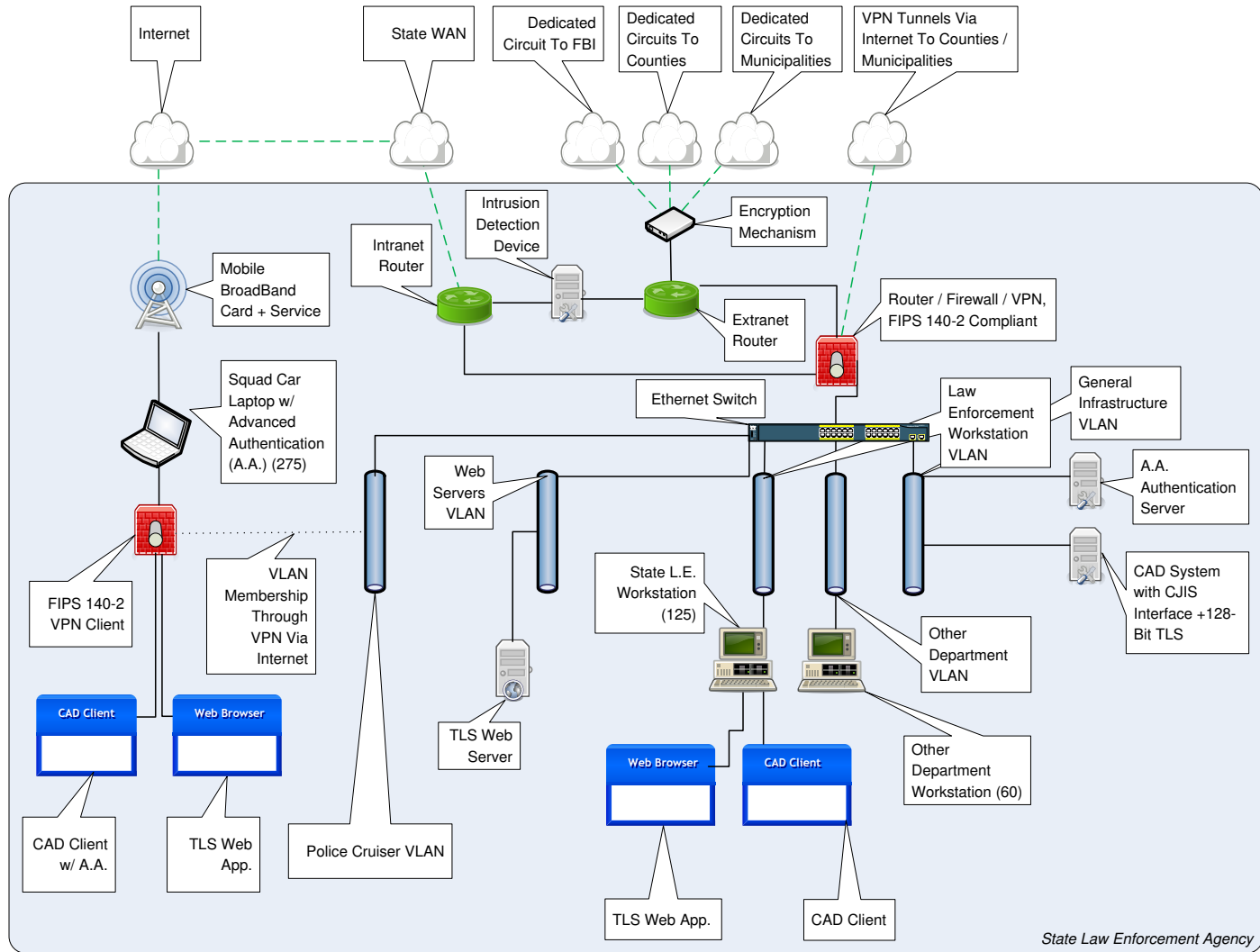


Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency

Conceptual Topology Diagram For A State Law Enforcement Agency



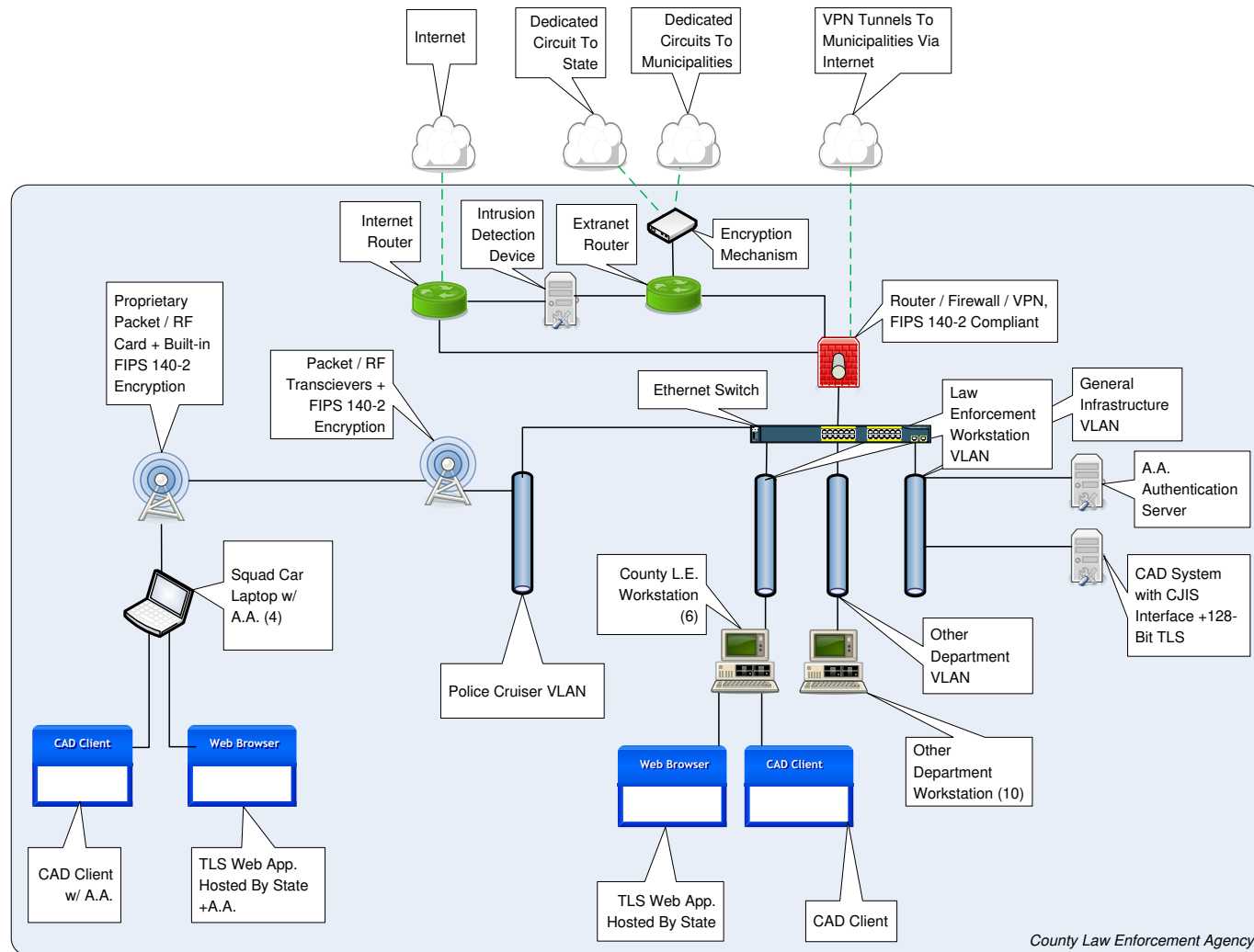
--- FIPS 140-2 COMPLIANT ENCRYPTION
 — STANDARD CONNECTION

Sample State Agency		
FOUO	01/01/2011	

Appendix C.1-B		
	01/01/2011	

Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency

Conceptual Topology Diagram For A County Law Enforcement Agency



--- FIPS 140-2 COMPLIANT ENCRYPTION
 — STANDARD CONNECTION

Sample County Agency

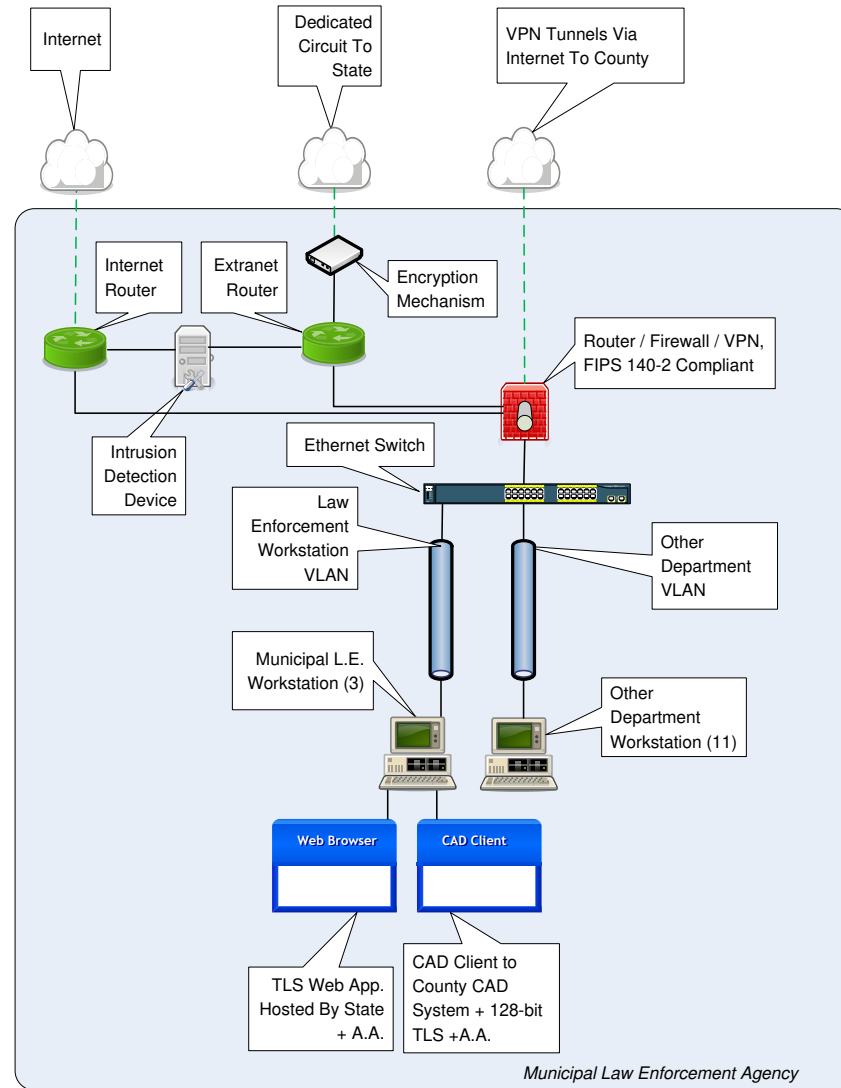
FOUO	01/01/2011	

Appendix C.1-C

01/01/2011

Figure C-1-D Conceptual Topology Diagram for a Municipal Law Enforcement Agency

Conceptual Topology Diagram For A Municipal Law Enforcement Agency



--- FIPS 140-2 COMPLIANT ENCRYPTION
 ——— STANDARD CONNECTION

Sample Municipal Agency		
FOUO	01/01/2011	

Appendix C.1-D		
	01/01/2011	

APPENDIX D SAMPLE INFORMATION EXCHANGE AGREEMENTS

D.1 CJIS User Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SYSTEMS USER AGREEMENT

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities, as well as the noncriminal justice community, for licensing and employment purposes. These services are administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEx); Law Enforcement Enterprise Portal; and the National Instant Criminal Background Check System (NICS).

The FBI CJIS Division provides the following services to its users, as applicable:

1. Operational, technical, and investigative assistance.
2. Telecommunication lines to state, federal, and regulatory interfaces.
3. Legal and legislative review of matters pertaining to all CJIS Systems.
4. Timely information on all aspects of all CJIS Systems and other related programs by means of operating manuals, code manuals, technical and operational updates, various newsletters, information letters, frequently asked questions, and other relevant documents.
5. Training assistance and up-to-date materials provided to each CSO, NICS Point of Contact (POC), state Compact Officer, State Administrator, Information Security Officer (ISO), and other appropriate personnel.
6. Ongoing assistance to Systems' users through meetings and briefings with the CSOs, State Administrators, Compact Officers, ISOs, and NICS State POCs to discuss operational and policy issues.
7. Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS programs.

8. National Crime Prevention and Privacy Compact Administrative Office through which states and other authorized users may submit issues concerning the noncriminal justice use of the III System.
9. Annual NICS Users Conference.
10. Audit.
11. Staff research assistance.

PART 1

The purpose behind a designated CSO is to unify responsibility for Systems user discipline and to ensure adherence to established procedures and policies within each signatory state/territory/tribal agency and by each federal user. This agreement outlines the responsibilities of each CSO as they relate to all CJIS Systems and other related CJIS administered programs. These individuals are ultimately responsible for planning necessary hardware, software, funding, and training for access to all CJIS Systems.

To ensure continued access as set forth above, the CSA agrees to adhere to all applicable CJIS policies including, but not limited to, the following:

1. The signatory state/tribal agency will provide fingerprints that meet submission criteria for all qualifying arrests. In addition, states/tribal agencies will make their records available for interstate exchange for criminal justice and other authorized purposes unless restricted by state/tribal law, and, where applicable, continue to move toward participation in the III and, upon ratification of the National Crime Prevention and Privacy Compact, the National Fingerprint File.
2. Appropriate and reasonable quality assurance procedures; e.g., hit confirmation, audits for record timeliness, and validation, must be in place to ensure that only complete, accurate, and valid information is maintained in the CJIS Systems.
3. Biannual file synchronization of information entered into the III by participating states.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history

records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

5. Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.
6. Training - Each agency shall be responsible for training requirements, including compliance with operator training mandates.
7. Integrity of the Systems - Each agency shall be responsible for maintaining the integrity of the system in accordance with FBI CJIS Division/state/federal/tribal policies to ensure only authorized terminal access; only authorized transaction submission; and proper handling and dissemination of CJI. Each agency shall also be responsible for computer security incident reporting as required by the *CJIS Security Policy*.

The following documents are incorporated by reference and made part of this agreement for CSA users:

1. Bylaws for the CJIS Advisory Policy Board and Working Groups.
2. CJIS Security Policy.
3. Interstate Identification Index Operational and Technical Manual, National Fingerprint File Operations Plan, NCIC 2000 Operating Manual, UCR Handbook-NIBRS Edition, and National Incident-Based Reporting System Volumes 1, 2, and 4.
4. National Crime Prevention and Privacy Compact, 42 United States Code (U.S.C.) §14616.
5. NCIC Standards and UCR Standards, as recommended by the CJIS Advisory Policy Board.
6. The National Fingerprint File Qualification Requirements.
7. Title 28, Code of Federal Regulations, Parts 20 and 25, §50.12, and Chapter IX.
8. Electronic Fingerprint Transmission Specifications.

9. Other relevant documents, to include: NCIC Technical and Operational Updates, CJIS Information Letters, NICS User Manual, NICS Interface Control Document.
10. Applicable federal, state, and tribal laws and regulations.

PART 2

Additionally, there are authorized federal regulatory recipients and other authorized users that provide electronic fingerprint submissions through a CJIS Wide Area Network (WAN) connection (or other approved form of electronic connection) to the CJIS Division that are required to comply with the following CJIS policies:

1. The authorized user will provide fingerprints that meet submission criteria and apply appropriate and reasonable quality assurance procedures.
2. Security - Each agency is responsible for appropriate security measures as applicable to physical security of communication equipment; personnel security to include background screening requirements; technical security to protect against unauthorized use; and security of criminal history records.
3. Audit - Each authorized user shall be responsible for complying with all audit requirements for CJIS Systems. Additionally, each authorized user is subject to a triennial audit by the CJIS Division Audit staff.
4. Training - Each authorized user receiving criminal history record information shall be responsible for training requirements, including compliance with proper handling of criminal history records.

The following documents are incorporated by reference and made part of this agreement for non-CSA authorized users:

1. CJIS Security Policy.
2. National Crime Prevention and Privacy Compact, 42 U.S.C. §14616.
3. Title 28, Code of Federal Regulations, Parts 20 and 25, § 50.12, and Chapter IX.
4. Other relevant documents, to include CJIS Information Letters.

5. Applicable federal, state, and tribal laws and regulations.

GENERAL PROVISIONS

Funding:

Unless otherwise agreed in writing, each party shall bear its own costs in relation to this agreement. Expenditures will be subject to federal and state budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

Termination:

1. All activities of the parties under this agreement will be carried out in accordance to the above-described provisions.
2. This agreement may be amended or terminated by the mutual written consent of the parties authorized representatives.
3. Either party may terminate this agreement upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:
 - a. The parties will continue participation, financial or otherwise, up to the effective date of termination.
 - b. Each party will pay the costs it incurs as a result of termination.
 - c. All information and rights therein received under the provisions of this agreement prior to the termination will be retained by the parties, subject to the provisions of this agreement.

ACKNOWLEDGMENT AND CERTIFICATION

As a CSO or CJIS WAN Official (or other CJIS authorized official), I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS Systems users to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained by means of, the CJIS Systems. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of sanctions against the offending state/agency; other federal, tribal, state, and local criminal justice users; and approved noncriminal justice users with System access, whether direct or indirect. The Director of the FBI (or the National Crime Prevention and Privacy Compact Council), may approve sanctions to include the termination of CJIS services.

I hereby certify that I am familiar with all applicable documents that are made part of this agreement and to all applicable federal and state laws and regulations relevant to the receipt and dissemination of documents provided through the CJIS Systems.

This agreement is a formal expression of the purpose and intent of both parties and is effective when signed. It may be amended by the deletion or modification of any provision contained therein, or by the addition of new provisions, after written concurrence of both parties. The "Acknowledgment and Certification" is being executed by the CSO or CJIS WAN Official (or other CJIS authorized official) in both an individual and representative capacity. Accordingly, this agreement will remain in effect after the CSO or CJIS WAN Official (or other CJIS authorized official) vacates his/her position or until it is affirmatively amended or rescinded in writing. This agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

SYSTEMS USER AGREEMENT

Please execute either Part 1 or Part 2

PART 1

Date: _____

CJIS Systems Officer

Printed Name/Title

CONCURRENCE OF CSA HEAD:

Date: _____

CSA Head

Printed Name/Title

PART 2

Date: _____

CJIS WAN Official (or other CJIS Authorized Official)

Printed Name/Title

CONCURRENCE OF CJIS WAN AGENCY HEAD:

Date: _____

CJIS WAN Agency Head

Printed Name/Title

FBI CJIS DIVISION:

Date: _____

[Name]

Assistant Director

FBI CJIS Division

* The FBI Designated Federal Officer should be notified when a CSO or other CJIS WAN/authorized Official vacates his/her position. The name and telephone number of the Acting CSO or other CJIS WAN/authorized Official, and when known, the name and telephone number of the new CSO or other CJIS WAN/authorized Official, should be provided. Revised: 05/03/2006

D.2 Management Control Agreement

Management Control Agreement

Pursuant to the CJIS Security Policy, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (Network Name) for the interstate exchange of criminal history/criminal justice information, the (Criminal Justice Agency) shall have the authority, via managed control, to set, maintain, and enforce:

- (1) Priorities.
- (2) Standards for the selection, supervision, and termination of personnel access to Criminal Justice Information (CJI).
- (3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
- (4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
- (5) Compliance with all rules and regulations of the (Criminal Justice Agency) Policies and CJIS Security Policy in the operation of all information received.

“...management control of the criminal justice function remains solely with the Criminal Justice Agency.” Section 5.1.1.4

This agreement covers the overall supervision of all (Criminal Justice Agency) systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any (Criminal Justice Agency) system to include NCIC Programs that may be subsequently designed and/or implemented within the (Criminal Justice Agency).

John Smith, CIO
Any State Department of Administration

Date

Joan Brown, CIO
(Criminal Justice Agency)

Date

D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

(Insert Name of Requesting Organization)

FOR

THE ESTABLISHMENT AND ACCOMMODATION OF
THIRD-PARTY CONNECTIVITY TO THE
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION'S WIDE AREA NETWORK

1. **PURPOSE:** This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI) and **(insert requesting organization's name)**, hereinafter referred to as the "parties," memorializes each party's responsibilities with regard to establishing connectivity to records services accessible via the Wide Area Network (WAN) of the FBI's Criminal Justice Information Services (CJIS) Division.

2. **BACKGROUND:** The requesting organization, **(insert requesting organization's name)**, being approved for access to systems of records accessible via the CJIS WAN, desires connectivity to the CJIS WAN or via a secure Virtual Private Network (VPN) Connection (Internet) to the CJIS WAN. The CJIS Division has created a framework for accommodating such requests based on the type of connection.

In preparing for such non-CJIS-funded connectivity to the CJIS WAN, the parties plan to acquire, configure, and place needed communications equipment at suitable sites and to make electronic connections to the appropriate systems of records via the CJIS WAN.

To ensure that there is a clear understanding between the parties regarding their respective roles in this process, this MOU memorializes each party's responsibilities regarding the development, operation, and maintenance of third-party connectivity to the CJIS WAN. Unless otherwise contained in an associated contract, the enclosed terms apply. If there is a conflict between terms and provisions contained in both the contract and this MOU, the contract will prevail.

3. **AUTHORITY:** The FBI is entering into this MOU under the authority provided by Title 28, United States Code (U.S.C.), Section 534; 42 U.S.C. § 14616; and/or Title 28, Code of Federal Regulations, Part 906.

4. SCOPE:

a. The CJIS Division agrees to:

i. Provide the requesting organization with a "CJIS WAN Third-Party Connectivity Package" that will detail connectivity requirements and options compatible with the CJIS Division's WAN architecture upon receipt of a signed nondisclosure statement.

ii. Configure the requesting organization's connection termination equipment suite at Clarksburg, West Virginia, and prepare it for deployment or shipment under the CJIS WAN option. In the Secure VPN arrangement only, the third party will develop, configure, manage, and maintain its network connectivity to its preferred service provider.

iii. Work with the requesting organization to install the connection termination equipment suite and verify connectivity.

iv. Perform installation and/or routine maintenance on the requesting organization's third-party dedicated CJIS WAN connection termination equipment after coordinating with the requesting organization's designated point of contact (POC) and during a time when the CJIS Division's technical personnel are near the requesting organization's site.

v. Perform periodic monitoring and troubleshooting of the requesting organization's CJIS WAN connection termination equipment. Software patches will be maintained on the dedicated CJIS WAN connected network equipment only. Under the Secure VPN option, no availability or data thru-put rates will be guaranteed.

vi. Provide 24 hours a day, 7 days a week uninterrupted monitoring from the CJIS Division's Network Operations Center.

vii. Provide information regarding potential hardware end-of-life replacement cycles to the requesting organization for its budgeting purposes.

viii. Maintain third-party dedicated CJIS WAN connection termination equipment as if in the CJIS Division's operational environment.

ix. Update the appropriate software on the requesting organization's dedicated connection termination equipment connected to the CJIS WAN (i.e., Cisco Internetwork Operating System, SafeNet frame relay encryptor firmware, etc.) pursuant to the requesting organization's authorized maintenance contracts.

x. Provide a POC and telephone number for MOU-related issues.

b. The **(insert requesting organization's name)** agrees to:

i. Coordinate requests for third-party connectivity to the CJIS WAN or the Secure VPN with the CJIS Division's POC.

ii. Purchase hardware and software that are compatible with the CJIS WAN.

iii. Pay for the telecommunications infrastructure that supports its connection to the CJIS WAN or Secure VPN.

iv. Maintain telecommunication infrastructure in support of Secure VPN connectivity.

v. Provide any/all hardware and software replacements and upgrades as mutually agreed to by the parties.

vi. Pay for all telecommunication requirements related to its connectivity.

vii. Provide required information for dedicated service relating to Data Link Connection Identifiers, Circuit Identifier, Permanent Virtual Circuit Identifiers, Local Exchange Carrier Identifier, POC, location, etc., as determined by the parties.

viii. Transport the CJIS WAN connection termination equipment suite to the CJIS Division for configuration and preparation for deployment under the dedicated service option.

ix. Provide registered Internet Protocol information to be used by the requesting organization's system to the CJIS Division.

x. Provide the CJIS Division with six months advance notice or stated amount of time for testing activities (i.e., disaster recovery exercises).

xi. Provide the CJIS Division with applicable equipment maintenance contract numbers and level of service verifications needed to perform software upgrades on connection termination equipment.

xii. Provide the CJIS Division with applicable software upgrade and patch images (or information allowing the CJIS Division to access such images).

xiii. Transport only official, authorized traffic over the Secure VPN.

xiv. Provide a POC and telephone number for MOU-related issues.

5. **FUNDING:** There are no reimbursable expenses associated with this level of support. Each party will fund its own activities unless otherwise agreed to in writing. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of understanding between the parties hereto of the nature of the relationship for the connectivity efforts. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditures.

6. **SETTLEMENT OF DISPUTES:** Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

7. SECURITY: It is the intent of the parties that the actions carried out under this MOU will be conducted at the unclassified level. No classified information will be provided or generated under this MOU.

8. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:

a. All activities of the parties under this MOU will be carried out in accordance with the above - described provisions.

b. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.

c. Either party may terminate this MOU upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

i. The parties will continue participation, financial or otherwise, up to the effective date of the termination.

ii. Each party will pay the costs it incurs as a result of the termination.

iii. All information and rights therein received under the provisions of this MOU prior to the termination will be retained by the parties, subject to the provisions of this MOU.

9. FORCE AND EFFECT: This MOU, which consists of nine numbered sections, will enter into effect upon signature of the parties and will remain in effect until terminated. The parties should review the contents of this MOU annually to determine whether there is a need for the deletion, addition, or amendment of any provision. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the parties.

FOR THE FEDERAL BUREAU OF INVESTIGATION

[Name]

Date

Assistant Director

Criminal Justice Information Services Division

FOR THE (insert requesting organization name)

Date

D.4 Interagency Connection Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)

Wide Area Network (WAN) USER AGREEMENT

BY INTERIM REMOTE LATENT USERS

The responsibility of the FBI CJIS Division is to provide state-of-the-art identification and information services to the local, state, federal, and international criminal justice communities, as well as the civil community for licensing and employment purposes. The data provided by the information systems administered and maintained by the FBI CJIS Division are routed to and managed in cooperation with the designated interface agency official. This information includes, but is not limited to, the Interstate Identification Index (III), National Crime Information Center (NCIC), Uniform Crime Reporting (UCR)/National Incident-Based Reporting System (NIBRS), and the Integrated Automated Fingerprint Identification System (IAFIS) programs.

In order to fulfill this responsibility, the FBI CJIS Division provides the following services to its users:

- Operational, technical, and investigative assistance;
- Telecommunications lines to local, state, federal and authorized interfaces;
- Legal and legislative review of matters pertaining to IAFIS, CJIS WAN and other related services;
- Timely information on all aspects of IAFIS, CJIS WAN, and other related programs by means of technical and operational updates, various newsletters, and other relative documents;
- Shared management through the CJIS Advisory Process and the Compact Council;
- Training assistance and up-to-date materials provided to each designated agency official, and;
- Audit.

The concept behind a designated interface agency official is to unify responsibility for system user discipline and ensure adherence to system procedures and policies within each interface agency. These individuals are ultimately responsible for planning necessary hardware, software, funding, training, and the administration of policy and procedures including security and integrity for complete access to CJIS related systems and CJIS WAN related data services by authorized agencies.

The following documents and procedures are incorporated by reference and made part of this agreement:

- *CJIS Security Policy*;
- *Title 28, Code of Federal Regulations, Part 20*;
- Computer Incident Response Capability (CIRC);
- Applicable federal and state laws and regulations.

To ensure continued access as set forth above, the designated interface agency agrees to adhere to all CJIS policies, including, but not limited to, the following:

1. The signatory criminal agency will provide fingerprints for all qualifying arrests either via electronic submission or fingerprint card that meet submission criteria. In addition, the agency will make their records available for interstate exchange for criminal justice and other authorized purposes.
2. The signatory civil agency with legislative authority will provide all qualifying fingerprints via electronic submission or fingerprint card that meet submission criteria.
3. Appropriate and reasonable quality assurance procedures must be in place to ensure that only complete, accurate, and valid information is maintained in the system.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunications lines; Interim Distributed Imaging System (IDIS) equipment shall remain stand-alone

devices and be used only for authorized purposes; personnel security to meet background screening requirements; technical security to protect against unauthorized use; data security, dissemination, and logging for audit purposes; and actual security of criminal history records. Additionally, each agency must establish an information security structure that provides for an Information Security Officer (ISO) or a security point of contact.

5. Audit - Each agency shall be responsible for complying with the appropriate audit requirements.
6. Training - Each agency shall be responsible for training requirements, including compliance with training mandates.
7. Integrity of the system shall be in accordance with FBI CJIS Division and interface agency policies. Computer incident reporting shall be implemented.

Until states are able to provide remote latent connectivity to their respective latent communities via a state WAN connection, the CJIS Division may provide direct connectivity to IAFIS via a dial-up connection or through the Combined DNA Index System (CODIS) and/or National Integrated Ballistics Information Network (NIBIN) connections. When a state implements a latent management system and is able to provide intrastate connectivity and subsequent forwarding to IAFIS, this agreement may be terminated. Such termination notice will be provided in writing by either the FBI or the state CJIS Systems Agency.

It is the responsibility of the local remote latent user to develop or acquire an IAFIS compatible workstation. These workstations may use the software provided by the FBI or develop their own software, provided it is IAFIS compliant.

The CJIS Division will provide the approved modem and encryptors required for each dial-up connection to IAFIS. The CJIS Communication Technologies Unit will configure and test the encryptors before they are provided to the user. Users requesting remote latent connectivity through an existing CODIS and/or NIBIN connection must receive verification from the FBI that there are a sufficient number of Ethernet ports on the router to accommodate the request.

If at any time search limits are imposed by the CJIS Division, these individual agency connections will be counted toward the total state allotment.

ACKNOWLEDGMENT AND CERTIFICATION

As a CJIS WAN interface agency official serving in the CJIS system, I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS system users in order to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in or obtained by means of the CJIS system. I further acknowledge that a failure to comply with these duties and responsibilities may subject our agency to various sanctions adopted by the CJIS Advisory Policy Board and approved by the Director of the FBI. These sanctions may include the termination of CJIS service.

As the designated CJIS WAN interface agency official serving in the CJIS system, I hereby certify that I am familiar with the contents of the *Title 28, Code of Federal Regulations, Part 20; CJIS Security Policy; Computer Incident Response Capability*; and applicable federal or state laws and regulations applied to IAFIS and CJIS WAN Programs for the dissemination of criminal history records for criminal and noncriminal justice purposes.

*

Signature

Print or Type

CJIS WAN Agency Official

Date

CONCURRENCE OF FEDERAL/REGULATORY AGENCY HEAD OR STATE CJIS SYSTEMS OFFICER (CSO):

*

Signature

Print or Type

*

Title

Date

State CSO

FBI CJIS DIVISION:

Signature – [Name]

Assistant Director

Title

Date

* If there is a change in the CJIS WAN interface agency official, the FBI Designated Federal Employee must be notified in writing 30 days prior to the change.

5/27/2004 UA modification reflects change in CTO title to CSO.

APPENDIX E SECURITY FORUMS AND ORGANIZATIONAL ENTITIES

Online Security Forums / Organizational Entities
AntiOnline
Black Hat
CIO.com
CSO Online
CyberSpeak Podcast
FBI Criminal Justice Information Services Division (CJIS)
Forrester Security Forum
Forum of Incident Response and Security Teams (FIRST)
Information Security Forum (ISF)
Information Systems Audit and Control Association (ISACA)
Information Systems Security Association (ISSA)
Infosyssec
International Organization for Standardization (ISO)
International Information Systems Security Certification Consortium, Inc. (ISC) ²
Metasploit
Microsoft Developer Network (MSDN) Information Security
National Institute of Standards and Technology (NIST)
Open Web Application Security Project (OWASP)
SANS (SysAdmin, Audit, Network, Security) Institute
SC Magazine
Schneier.com
Security Focus
The Register
US Computer Emergency Response Team (CERT)
US DoJ Computer Crime and Intellectual Property Section (CCIPS)

APPENDIX F SAMPLE FORMS

This appendix contains sample forms.

F.1 Security Incident Response Form

**FBI CJIS DIVISION
INFORMATION SECURITY OFFICER (ISO)
SECURITY INCIDENT REPORTING FORM**

NAME OF PERSON REPORTING THE INCIDENT: _____

DATE OF REPORT: _____ (mm/dd/yyyy)

DATE OF INCIDENT: _____ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): _____

LOCATION(S) OF INCIDENT: _____

INCIDENT DESCRIPTION: _____

SYSTEM(S) AFFECTED: _____

SYSTEM(S) AFFECTED (e.g. CAD, RMS, file server, etc.): _____

METHOD OF DETECTION: _____

ACTIONS TAKEN/RESOLUTION: _____

Copies To:

John C. Weatherly

(FBI CJIS Division ISO)

1000 Custer Hollow Road

Clarksburg, WV 26306-0102

(304) 625-3660

iso@fbi.gov

APPENDIX G BEST PRACTICES

G.1 Virtualization

Virtualization

This appendix documents security considerations for implementing and operating virtual environments that process, store, and/or transmit Criminal Justice Information.

The FBI CJIS ISO has fielded several inquiries from various states requesting guidance on implementing virtual environments within their data centers. With the proliferation of virtual environments across industry in general there is a realistic expectation that FBI CJIS Auditors will encounter virtual environments during the upcoming year. Criminal Justice Agencies (CJAs) and Noncriminal Justice Agencies (NCJAs) alike need to understand and appreciate the foundation of security protection measures required for virtual environments.

From Microsoft's Introduction to Windows Server 2008

<http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx>:

"Server virtualization, also known as hardware virtualization, is a hot topic in the IT world because of the potential for serious economic benefits. Server virtualization enables multiple operating systems to run on a single physical machine as virtual machines (VMs). With server virtualization, you can consolidate workloads across multiple underutilized server machines onto a smaller number of machines. Fewer physical machines can lead to reduced costs through lower hardware, energy, and management overhead, plus the creation of a more dynamic IT infrastructure."

From a trade publication, kernelthread.com

<http://www.kernelthread.com/publications/virtualization/>:

"Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others."

From an Open Source Software developer

<http://www.kallasoft.com/pc-hardware-virtualization-basics/>:

"Virtualization refers to virtualizing hardware in software, allowing multiple operating systems, or images, to run concurrently on the same hardware. There are two main types of virtualization software:

- *"Type-1 Hypervisor, which runs 'bare-metal' (on top of the hardware)*
- *"Type-2 Hypervisor which requires a separate application to run within an operating system*

“Type1 hypervisors usually offer the best in efficiency, while Type-2 hypervisors allow for greater support of hardware that can be provided by the operating system. For the developer, power user, and small business IT professionals, virtualization offers the same basic idea of collapsing multiple physical boxes into one. For instance, a small business can run a web server and an Exchange server without the need for two boxes. Developers and power users can use the ability to contain different development environments without the need to modify their main operating system. Big businesses can also benefit from virtualization by allowing software maintenance to be run and tested on a separate image on hardware without having to take down the main production system.”

Industry leaders and niche developers are bringing more products to market every day. The following article excerpts, all posted during September 2008, on www.virtualization.com are examples of industry offerings.

“Microsoft and Novell partnered together for joint virtualization solution. Microsoft and Novell are announcing the availability of a joint virtualization solution optimized for customers running mixed-source environments. The joint offering includes SUSE Linux Enterprise Server configured and tested as an optimized guest operating system running on Windows Server 2008 Hyper-V, and is fully supported by both companies’ channel partners. The offering provides customers with the first complete, fully supported and optimized virtualization solution to span Windows and Linux environments.”

“Sun Microsystems today announce the availability of Sun xVM Server software and Sun xVM Ops Center 2.0, key components in its strategy. Sun also announced the addition of comprehensive services and support for Sun xVM Server software and xVM Ops Center 2.0 to its virtualization suite of services. Additionally, Sun launched xVMserver.org, a new open source community, where developers can download the first source code bundle for Sun xVM Server software and contribute to the direction and development of the product.”

“NetEx, specialist in high-speed data transport over TCP, today announced Virtual HyperIP bandwidth optimization solutions for VMware environments that deliver a threefold to tenfold increase in data replication performance. Virtual HyperIP is a software-based Data Transport Optimizer that operates on the VMware ESX server and boosts the performance of storage replication applications from vendors such as EMC, NetApp, Symantec, IBM, Data Domain, and FalconStor. Virtual HyperIP mitigates TCP performance issues that are common when moving data over wide-area network (WAN) connections because of bandwidth restrictions, latency due to distance and/or router hop counts, packet loss and network errors. Like the company’s award-winning appliance-based HyperIP, Virtual HyperIP eliminates these issues with an innovative software design developed specifically to accelerate traffic over an IP based network.”

From several sources, particularly:

<http://www.windowsecurity.com/articles/security-virtualization.html>

<http://csrc.nist.gov/publications/drafts/6--64rev2/draft-sp800-64-Revision2.pdf>

Virtualization provides several benefits:

- Make better use of under-utilized servers by consolidating to fewer machines saving on hardware, environmental costs, management, and administration of the server infrastructure.
- Legacy applications unable to run on newer hardware and/or operating systems can be loaded into a virtual environment – replicating the legacy environment.
- Provides for isolated portions of a server where trusted and untrusted applications can be ran simultaneously – enabling hot standbys for failover.
- Enables existing operating systems to run on shared memory multiprocessors.
- System migration, backup, and recovery are easier and more manageable.

Virtualization also introduces several vulnerabilities:

- Host Dependent.
- If the host machine has a problem then all the VMs could potentially terminate.
- Compromise of the host makes it possible to take down the client servers hosted on the primary host machine.
- If the virtual network is compromised then the client is also compromised.
- Client share and host share can be exploited on both instances. Potentially this can lead to files being copied to the share that fill up the drive.

These vulnerabilities can be mitigated by the following factors:

- Apply “least privilege” technique to reduce the attack surface area of the virtual environment and access to the physical environment.
- Configuration and patch management of the virtual machine and host, i.e. Keep operating systems and application patches up to date on both virtual machines and hosts.
- Install the minimum applications needed on host machines.
- Practice isolation from host and virtual machine.
- Install and keep updated antivirus on virtual machines and the host.
- Segregation of administrative duties for host and versions.
- Audit logging as well as exporting and storing the logs outside the virtual environment.
- Encrypting network traffic between the virtual machine and host IDS and IPS monitoring.
- Firewall each virtual machine from each other and ensure that only allowed protocols will transact.

G.2 Voice over Internet Protocol

Voice over Internet Protocol (VoIP)

Attribution:

The following information has been extracted from NIST Special Publication 800-58, Security Considerations for Voice over IP Systems.

Definitions:

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Summary:

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are alluring since the typical cost to operate VoIP is less than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol services. Unfortunately, installing a VoIP network is not a simple "plug-and-play" procedure. There are myriad security concerns, cost issues with new networking hardware requirements, and overarching quality of service (QoS) factors that have to be considered carefully.

What are some of the advantages of VoIP?

- a. Cost – a VoIP system is usually cheaper to operate than an equivalent office telephone system with a Private Branch Exchange and conventional telephone service.
- b. Integration with other services – innovative services are emerging that allow customers to combine web access with telephone features through a single PC or terminal. For example, a sales representative could discuss products with a customer using the company's web site. In addition, the VoIP system may be integrated with video across the Internet, providing a teleconferencing facility.

What are some of the disadvantages of VoIP?

- a. Startup cost – although VoIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VoIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VoIP field develops.
- b. Security – the flexibility of VoIP comes at a price: added complexity in securing voice and data. Because VoIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VoIP system than a conventional voice telephone system or PBX.

VoIP Risks, Threats, and Vulnerabilities

This section details some of the potential threats and vulnerabilities in a VoIP environment, including vulnerabilities of both VoIP phones and switches. Threat discussion is included because the varieties of threats faced by an organization determine the priorities in securing its communications equipment. Not all threats are present in all organizations. A commercial firm may be concerned primarily with toll fraud, while a government agency may need to prevent disclosure of sensitive information because of privacy or national security concerns. Information security risks can be broadly categorized into the following three types: confidentiality, integrity, and availability, (which can be remembered with the mnemonic “CIA”). Additional risks relevant to switches are fraud and risk of physical damage to the switch, physical network, or telephone extensions.

Packet networks depend for their successful operation on a large number of configurable parameters: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as Call Managers and other programs used to place and route calls. Many of these network parameters are established dynamically every time a network component is restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

Vulnerabilities described in this section are generic and may not apply to all systems, but investigations by NIST and other organizations have found these vulnerabilities in a number of VoIP systems. In addition, this list is not exhaustive; systems may have security weaknesses that are not included in the list. For each potential vulnerability, a recommendation is included to eliminate or reduce the risk of compromise.

Confidentiality and Privacy

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes confidential memoranda, financial information, and security information such as passwords. In a telecommunications switch, eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and denial of service attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker’s job easier.

With conventional telephones, eavesdropping usually requires either physical access to tap a line, or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network.

Switch Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. This vulnerability also allows for wiretapping conversations on the network with port mirroring or bridging. An attacker with access to the switch administrative interface can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications. Failing to change default passwords is one of the most common errors made by inexperienced users.

REMEDIATION: If possible, remote access to the graphical user interface should be disabled to prevent the interception of plaintext administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface. Disabling port mirroring on the switch should also be considered.

Classical Wiretap Vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment makes it easy to intercept voice traffic.

REMEDIATION: A good physical security policy for the deployment environment is a general first step to maintaining confidentiality. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

ARP Cache Poisoning and ARP Floods

Because many systems have little authentication, an intruder may be able to log onto a computer on the VoIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic, then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation eavesdropping. Broadcasting ARP replies blind is sufficient to corrupt many ARP caches. Corrupting the ARP cache makes it possible to re-route traffic to intercept voice and data traffic.

REMEDIATION: Use authentication mechanisms wherever possible and limit physical access to the VoIP network segment.

Web Server interfaces

Both VoIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plaintext HTTP packets to gain confidential information. This would require access to the local network on which the server resides.

REMEDIATION: If possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

IP Phone Netmask Vulnerability

A similar effect of the ARP Cache Vulnerability can be achieved by assigning a subnet mask and router address to the phone crafted to cause most or all of the packets it transmits to be sent to an attacker's MAC address. Again, standard IP forwarding makes the intrusion all but undetectable.

REMEDIATION: A firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

Extension to IP Address Mapping Vulnerability

Discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's job may be much more difficult to accomplish and require much longer, possibly resulting in the attack being discovered.

REMEDIATION: Disabling the hub on the IP Phone will prevent this kind of attack. However, it is a rather simple task to turn the hub back on.

Integrity Issues

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator. Telecommunication switches must protect the integrity of their system data and configuration. Because of the richness of feature sets available on switches, an attacker who can compromise the system configuration can accomplish nearly any other goal. For example, an ordinary extension could be re-assigned into a pool of phones that supervisors can listen in on or record conversations for quality control purposes. Damaging or deleting information about the IP network used by a VoIP switch results in an immediate denial of service.

The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for intruders to use on their next visit. For this reason, the security system must be carefully protected. Integrity threats include any in which system functions or data may be corrupted, either accidentally or as a result of malicious actions. Misuse may involve legitimate users (i.e. insiders performing unauthorized operations) or intruders.

A legitimate user may perform an incorrect, or unauthorized, operations function (e.g., by mistake or out of malice) and may cause deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

Intrusion - An intruder may masquerade as a legitimate user and access an operations port of the switch. There are a number of serious intrusion threats. For example, the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion (e.g., modifying the security log) so that it may not be readily detected

Insecure state - At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

- After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, even though new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.
- At the time of installation the switch may be vulnerable until the default security features have been replaced.

DHCP Server Insertion Attack

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information.

This attack allows for possible man in the middle attacks on the IP-media gateway, and IP Phones. Many methods exist with the potential to reboot the phone remotely, e.g. “social engineering”, ping flood, MAC spoofing (probably SNMP hooks, etc.).

REMEDIATION: If possible, use static IP addresses for the IP Phones. This will remove the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing this traffic only from the legitimate server.

TFTP Server Insertion Attack

It is possible to change the configuration of a target phone by exploiting the TFTP response race when the IP phone is resetting. A rogue TFTP server can supply spurious

information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone.

REMEDIATION: Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VoIP systems should look for IP Phone instruments that can download signed binary files.

Availability and Denial of Service

Availability refers to the notion that information and services be available for use when needed. Availability is the most obvious risk for a switch. Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration or even denial of service or functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service. A voice over IP system may have additional vulnerabilities with Internet connections. Because intrusion detection systems fail to intercept a significant percentage of Internet based attacks, attackers may be able to bring down VoIP systems by exploiting weaknesses in Internet protocols and services.

Any network may be vulnerable to denial of service attacks, simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

CPU Resource Consumption Attack without any account information.

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, which would introduce intrusion vulnerabilities.

REMEDIATION: The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. Similarly, VoIP telephones often have default keypad sequences that can be used to unlock and modify network information.

This vulnerability would allow an attacker to control the topology of the network remotely, allowing for not only complete denial of service to the network, but also a port mirroring attack to the attacker's location, giving the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface, providing an attacker with the ability to disrupt the network without advance knowledge of switch operations and commands. In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an attacker could substitute another IP address pointing to a call manager that would allow eavesdropping or traffic analysis.

REMEDIATION: Changing the default password is crucial. Moreover, the graphical user interface should be disabled to prevent the interception of plaintext administration sessions.

Exploitable software flaws

Like other types of software, VoIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities: denial of service or revelation of critical system parameters. Denial of service can often be implemented remotely, by passing packets with specially constructed headers that cause the software to fail. In some cases the system can be crashed, producing a memory dump in which an intruder can find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that allow the introduction of malicious code have been found in VoIP software, as in other applications.

REMEDIATION: These problems require action from the software vendor, and distribution of patches to administrators. Intruders monitor announcements of vulnerabilities, knowing that many organizations require days or weeks to update their software. Regular checking for software updates and patches is essential to reducing these vulnerabilities. Automated patch handling can assist in reducing the window of opportunity for intruders to exploit known software vulnerabilities.

Account Lockout Vulnerability

An attacker will be able to provide several incorrect login attempts at the telnet prompt until the account becomes locked out. (This problem is common to most password-protected systems, because it prevents attackers from repeating login attempts until the correct password is found by trying all possible combinations.)

The account is unable to connect to the machine for the set lockout time.

REMEDIATION: If remote access is not available, this problem can be solved with physical access control.

NIST Recommendations.

Because of the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. In particular, start with these general guidelines, recognizing that practical considerations, such as cost or legal requirements, may require adjustments for the organization:

1. Develop appropriate network architecture.

- Separate voice and data on logically different networks if feasible. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection at the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients towards a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help.
- A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways (ALGs) for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature.
- Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied, e.g., H.235 Annex D for integrity provision or TLS to protect SIP signaling).
- Use IPsec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.
- If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide Advanced Encryption System (AES) encryption at reasonable cost. Note that Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer

and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

2. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.

VoIP can provide more flexible service at lower cost, but there are significant tradeoffs that must be considered. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack (see VoIP Risks, Threats, and Vulnerabilities section for more detailed discussion of vulnerabilities of VoIP and their relation to data network vulnerabilities).

Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

3. Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

Unlike traditional telephone connections, which are tied to a physical location, VoIP's packet switched technology allows a particular number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the tradeoff is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Agencies must carefully evaluate E-911 issues in planning for VoIP deployment.

4. Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect with a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are communicating). Agencies therefore should ensure that adequate physical security is in place to restrict access to VoIP network components. Physical security measures, including barriers, locks, access control systems, and guards, are the first line of defense. Agencies must make sure that the proper physical countermeasures are in place to mitigate some of

the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking this means that installation of a sniffer could result in not just data but all voice communications being intercepted.

5. VoIP-ready firewalls and other appropriate protection mechanisms should be employed. Agencies must enable, use, and routinely test the security features that are included in VoIP systems.

Because of the inherent vulnerabilities (e.g. susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

6. If practical, “softphone” systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern.

Worms, viruses, and other malicious software are extraordinarily common on PCs connected to the internet, and very difficult to defend against. Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user’s knowledge, even if the user does nothing more than visit a compromised web site. Malicious software attached to email messages can also be installed without the user’s knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of “softphones”, for most applications. In addition, because PCs are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

7. If mobile units are to be integrated with the VoIP system, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent WiFi Protected Access (WPA), a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid the integration of wireless technology with VoIP. NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for Federal agencies that have determined that certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

8. Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone systems. Agencies should review these issues with their legal advisors. See Section 2.5 for more on these issues.

G.3 Cloud Computing

Cloud Computing

Purpose:

This paper is provided to define and describe cloud computing, discuss CJIS Security Policy (CSP) compliance, detail security and privacy, and provide general recommendations.

Attribution:

- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (Dec. 2011)
- NIST SP 800-145, the NIST Definition of Cloud Computing (Sept. 2011)
- NIST SP 800-146, Cloud Computing Synopsis and Recommendations (May 2011)
- CJIS Security Policy, Version 5.0

Definitions and Terms:

Cloud computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), software, and information.

Cloud subscriber – A person or organization that is a customer of a cloud

Cloud client – A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a subscriber

Cloud provider – An organization that provides cloud services

Summary:

With many law enforcement agencies looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing to maintain data and applications is a viable business solution. But the unique security and legal characteristics of law enforcement agencies means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be with access to the FBI's CJIS systems and the protection of Criminal Justice Information (CJI), security and policy compliance concerns are bound to arise.

Cloud computing has become a popular and sometimes contentious topic of discussion for both the private and public sectors. This is in part because of the difficulty in describing cloud computing in general terms, because it is not a single kind of system. The “cloud” spans a spectrum of underlying technologies, configuration possibilities, service and deployment models. Cloud computing offers the ability to conveniently rent access to fully featured applications, software development and deployment environments, and computing infrastructure assets - such as network-accessible data storage and processing from a cloud service provider.

One of the benefits of cloud computing is the ability to outsource many of the technical functions agencies may not want to perform for various reasons. Ultimately, the move to cloud computing is a business and security risk decision in which the following relevant factors are given proper consideration:

- readiness of existing applications for cloud deployment
- transition costs
- life-cycle costs
- maturity of service orientation in existing infrastructure
- security and privacy requirements – federal, state, and local

Achieving CJIS Security Policy Compliance:

The question that is often asked is, “Can an Agency be compliant with the CJIS Security Policy and also cloud compute?”

Because the CJIS Security Policy is device and architecture independent (per CSP Section 2.2), the answer is yes, and this can be accomplished— assuming the vendor of the cloud technology is able to meet the existing requirements of the CJIS Security Policy.

There are security challenges that must be addressed if CJI is to be sent into or through, stored within, or accessed from the cloud.

Admittedly, the existing CJIS Security Policy requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel; however, the requirements aren’t new to vendors serving the criminal justice community and many vendors have been successfully meeting the Policy requirements for years. Even so, they are the minimum security requirements which will provide an acceptable level of assurance that law enforcement and personally identifiable information (PII) will be protected when shared with other law enforcement agencies across the nation.

General CJIS Security Policy Applicability Questions

Before tackling these challenges, the cloud subscriber should first be aware of what security and legal requirements they are subject to prior to entering into any agreement with a cloud provider. Asking the following general questions will help frame the process of determining compliance with the existing requirements of the CJIS Security Policy.

- Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)
- Will advanced authentication (AA) be required for access to CJI within a cloud environment? (5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale)
- Does/do any cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9.1 Physically Secure Location)
- Are the encryption requirements being met? (5.10.1.2 Encryption)
 - Who will be providing the encryption as required in the CJIS Security Policy (client or cloud service provider)? *Note: individuals with access to the keys can decrypt the stored files and therefore have access to unencrypted CJI.*
 - Is the data encrypted while at rest and in transit?
- What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response)
 - Will the cloud subscriber be notified of any incident?
 - If CJI is compromised, what are the notification and response procedures?
- Is the cloud service provider a private contractor/vendor?
 - If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI? (5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors)
- Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? *Note: Cloud facilities such as datacenters in which CJI will be stored or processed should be audited as would any other datacenter housing and processing CJI.* (5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)

- How will event and content logging be handled? (5.4 Policy Area 4, Auditing and Accountability)
 - Will the cloud service provider handle the events and content logging required by the CJIS Security Policy and provide that upon request?
 - What are the cloud service provider's responsibilities with regard to media protection and destruction? (5.8 Policy Area 8: Media Protection)

Ultimately, the goal is to remain committed to using technology in its information sharing processes, but not at the sacrifice of the security of the information with which it has been entrusted. As stated in the CJIS Security Policy, device and architecture independence permits the use of cloud computing, but the security requirements do not change.

Cloud Utilization Scenarios

1. Encrypted CJI in a Cloud Environment–Key Management Control, Security Awareness Training, and Personnel Controls

Prior to permitting CJI to be stored or traverse through a cloud environment, the agency should ensure proper encryption key management control procedures are implemented to determine who has access and control over the encryption keys. Proper key management control is vital to CJI security as those individuals (agency or cloud employees) with access to the keys can decrypt the stored files, and therefore, have unescorted access to unencrypted CJI. This means all those individuals must be subjected to security awareness training (CJIS Security Policy section 5.2) and must meet personnel security (CJIS Security Policy Section 5.12) requirements as individuals with unescorted access to unencrypted CJI.

Note: As a best security practice, the CJIS ISO Program does not recommend allowing the cloud service provider access to the encryption keys used to protect CJI. However, it may not always be reasonable to expect the agency, criminal justice or noncriminal justice, to accomplish this task.

- a. Scenario 1–Agency Stores CJI in a Cloud:

A CJA stores encrypted CJI (Backup files and drives) in a cloud service provider's environment. To access CJI, the agency will extract the CJI from the cloud to its local machine, and then decrypt the CJI. The CJI is processed, re-encrypted, and then re-uploaded to the cloud environment for storage. In this scenario, the agency always encrypts the CJI prior to placing it in the cloud and only authorized users of the agency have access to the encryption keys. Since the agency maintains the encryption keys, the cloud service provider employees would not need to undergo fingerprint-based background checks, nor have security awareness training. These requirements are negated, because only authorized personnel with access to the keys have the ability to view this CJI in an unencrypted form.

- b. Scenario 2–Agency Accesses CJI While in a Cloud:

A CJA stores CJI (files and drives) in a cloud service provider's environment, but as part of daily operations authorized users will remotely access the encrypted CJI in the cloud. The user will decrypt the CJI while it is in the cloud's virtual environment, process the data, and then re-encrypt the data prior to ending the remote session. The agency maintains the keys and the cloud service provider does not have access to the encryption keys. However, since the CJI is decrypted within the cloud's virtual environment, any administrative personnel employed by the cloud provider having the ability to access the virtual environment must be identified and subjected to security awareness training and personnel security controls as described in the CJIS Security Policy.

c. Scenario 3—CJI Impact from a Cloud Datacenter Critical Systems Crash—Core Dump² Recovery:

A CJA utilizes a cloud service provider (IaaS or PaaS) to store CJI and remotely accesses the environment to process CJI. During normal operation, the cloud provider experiences systems outages within the datacenter in which CJI is processed and stored. The cloud provider's administrators need to repair the systems and restore service using data from a core dump to return to normal operations. The cloud service provider as part of the Service Level Agreement (SLA) with the CJA has been authorized to maintain the encryption keys in order respond to such an event. The cloud administrators with such access have underwent fingerprint-based background checks and security awareness training. This allows the cloud administrators to decrypt CJI so that it is written to the core dump files for restoration following the system outage. CJI, however, is encrypted at all times except when part of the core dump files. As part of the SLA, the cloud service provider has agreed to treat the core dump files as CJI to ensure all protection are in place in compliance with the CJIS Security Policy.

Note: Writing encrypted data to a core dump corrupts the data and makes it unusable because the key no longer decrypts the data. This is problematic when attempting to recover encrypted data written to a core dump. The CJA could have ensured the cloud provider exclude encrypted data (CJI) from the core dump, but chose against it.

The Cloud Model Explained:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

² Core Dump - A file of a computer's documented memory of when a program or computer crashed. The file consists of the recorded status of the working memory at an explicit time, usually close to when the system crashed or when the program ended atypically as it presents the risk that the system failure would ensure the loss of the encrypted data.

The cloud model as defined by NIST consists of five essential characteristics, offers the option of three service models, and may be deployed via any of four deployment models as shown in Figure 1 below:

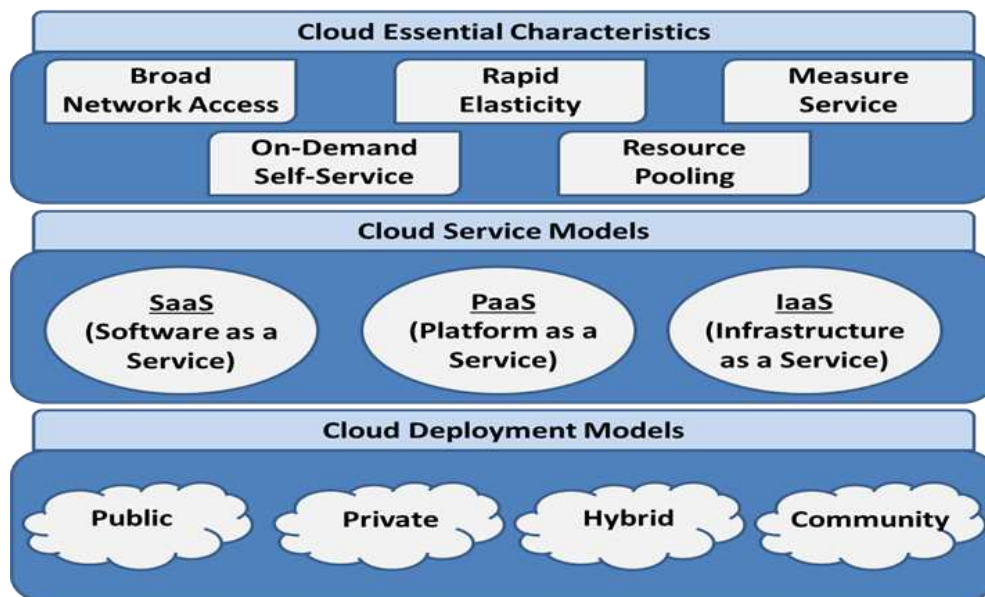


Figure 1 - Visual Depiction of the NIST Cloud Computing Definition

Essential Characteristics:

On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in which the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction

(e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability* at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

** Typically this is done on a pay-per-use or charge-per-use basis.*

Deployment Models:

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Service Models:

Software as a Service (SaaS)

This model provides the consumer the capability to use the provider's applications running on a cloud infrastructure*.

** A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.*

The SaaS service model is often referred to as “Software deployed as a hosted service and accessed over the Internet.”

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

When using the SaaS service model it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS)

This model provides the consumer the capability to deploy consumer-created or acquired applications* created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure.

** This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.*

When using the PaaS service model the consumer may have control over the deployed applications and possibly configuration settings for the application-hosting environment, but does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

Infrastructure as a Service (IaaS)

This model provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications.

When using the IaaS service model the consumer may have control over operating systems, storage, and deployed applications; and possibly limited control of select

networking components (e.g., host firewalls), but does not manage or control the underlying cloud infrastructure.

Key Security and Privacy Issues:

Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models.

Because cloud computing has grown out of an amalgamation of technologies, including service oriented architecture, virtualization, Web 2.0, and utility computing, many of the privacy and security issues involved can be viewed as known problems cast in a new setting. The importance of their combined effect in this setting, however, should not be discounted. Public cloud computing does represent a thought-provoking paradigm shift from conventional norms to an open organizational infrastructure—at the extreme, *displacing applications from one organization's infrastructure to the infrastructure of another organization, where the applications of potential adversaries may also operate.*

Governance

Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

Dealing with cloud services requires attention to the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met. Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with cloud computing. Audit mechanisms and tools should be in place to determine how data is stored, protected, and used, to validate services, and to verify policy enforcement. A risk management program should also be in place that is flexible enough to deal with the continuously evolving and shifting risk landscape.

Compliance

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.

Law and Regulations

Cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy. However, the degree to which they will accept liability in their service agreements, for exposure of content under their control, remains to be seen. Even so, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

Data Location

One of the most common compliance issues facing an organization is data location. A characteristic of many cloud computing services is that data is stored redundantly in multiple physical locations and detailed information about the location of an organization's data is unavailable or not disclosed to the service consumer. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. External audits and security certifications can alleviate this issue to some extent, but they are not a panacea.

When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations.

Electronic Discovery

The capabilities and processes of a cloud provider, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner. A cloud provider's archival capabilities may not preserve the original metadata as expected, causing spoliation (i.e., the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation), which could negatively impact litigation.

Trust

Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and privacy, and in doing so, confers a high level of trust onto the cloud provider. At the same time, federal agencies have a responsibility to protect information and information systems commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction, regardless of whether the information is collected or maintained by or on behalf of the agency; or whether the information systems are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

Insider Access

Data processed or stored outside the physical confines of an organization, its firewall, and other security controls bring with it an inherent level of risk. The insider security threat is a well-known issue for most organizations. Incidents may involve various types of fraud, sabotage of information resources, and theft of sensitive information.

Data Ownership

The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust and privacy of data. The continuing controversy over privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved.

Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

Visibility

Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Transition to public cloud services entails a transfer of responsibility to the cloud provider for securing portions of the system on which the organization's data and applications operate.

Ancillary Data

While the focus of attention in cloud computing is mainly on protecting application data, cloud providers also hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks.

Risk Management

Assessing and managing risk in systems that use cloud services can be a challenge. With cloud-based services, some subsystems or subsystem components fall outside of the direct control of a client organization. Many organizations are more comfortable with risk when they have greater control over the processes and equipment involved. Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls. Ultimately, if the level of trust in the service falls below expectations and the organization is unable to employ compensating controls, it must either reject the service or accept a greater degree of risk.

Architecture

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. It is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. With such information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to assess and manage risk.

Identity and Access Management

Data sensitivity and privacy of information have become increasingly an area of concern for organizations. The identity proofing and authentication aspects of identity management entail the use, maintenance, and protection of PII collected from users. Preventing unauthorized access to information resources in the cloud is also a major consideration. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove difficult.

Software Isolation

High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost

benefits and efficiencies due to economies of scale. Regardless of the service model and multi-tenant software architecture used, the computations of different consumers must be able to be carried out in isolation from one another, mainly through the use of logical separation mechanisms.

Data Protection

Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds.

Value Concentration

Having data collocated with that of an organization with a high threat profile could also lead to a denial of service, as an unintended casualty from an attack targeted against that organization. Similarly, side effects from a physical attack against a high profile organization's cloud-based resources are also a possibility. For example, over the years, facilities of the Internal Revenue Service have attracted their share of attention from would-be attackers.

Data Isolation

Database environments used in cloud computing can vary significantly. Accordingly, various types of multi-tenant arrangements exist for databases. Each arrangement pools resources differently, offering different degrees of isolation and resource efficiency. Regardless of implementation decision, data must be secured while at rest, in transit, and in use, and access to the data must be controlled.

Data Sanitization

The data sanitization practices that a cloud provider implements have obvious implications for security. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to prevent unauthorized disclosure of information. Data sanitization also applies to backup copies made for recovery and restoration of service and residual data remaining upon termination of service.

In a public cloud computing environment, data from one consumer is physically collocated (e.g., in an IaaS data store) or commingled (e.g., in a SaaS database) with the data of other consumers, which can complicate matters. Service agreements should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle.

Encryption

Client end-to-end encryption (e.g. encryption/decryption occurs on the law enforcement controlled client prior to data entering the cloud and decryption occurs only on the client device after encrypted data is removed from the cloud service) with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data.

- May cause significant cloud service functionality limitations on available service types made available for sensitive data. This may also increase expenses to cover key items, such as key management and client software. Additionally, a number of specific SLA or contract clauses may be necessary for the implementation of client end-to end encryption.

Use of cloud services without end-to-end encryption implemented by the client is another option that would require cloud service provider participation in the encryption of data.

- This would require at least some cloud provider personnel to undergo personnel background screening and training.
- Specialized Service Level Agreements (SLA) and/or contractual clauses would be necessary to identify those personnel that may have access to unencrypted, sensitive data.
- Conducting the analysis and gaining approval of particular cloud service implementations not utilizing end-to-end encryption for sensitive law enforcement data may be costly and time consuming due to the high degree of technical complexity.

Availability

In simple terms, availability is the extent to which an organization's full set of computational resources is accessible and usable. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. The concern is that most downtime is unplanned and can impact the mission of the organization. Some examples of unplanned service interruptions that cause concerns are:

- Temporary Outages
- Prolonged and Permanent Outages
- Denial of Service

Incident Response

The complexity of a cloud service can obscure recognition and analysis of incidents. Revising an organization's incident response plan to address differences between the organizational computing environment and a cloud computing environment is an important, but easy-to-overlook prerequisite to transitioning applications and data.

Data Availability

The availability of relevant data from event monitoring is essential for timely detection of security incidents. Cloud consumers are often confronted with extremely limited capabilities for detection of incidents in public cloud environments. The situation varies among cloud service models and cloud providers. For example, PaaS providers typically do not make event logs available to consumers, who are then left mainly with event data from self-deployed applications (e.g., via application logging). Similarly, SaaS consumers are completely dependent upon the cloud provider to provide event data such as activity logging, while IaaS consumers control more of the information stack and have access to associated event sources.

Incident Analysis and Resolution

An analysis to confirm the occurrence of an incident or determine the method of exploit needs to be performed quickly and with sufficient detail of documentation and care to ensure that traceability and integrity is maintained for subsequent use, if needed (e.g., a forensic copy of incident data for legal proceedings). Issues faced by cloud consumers when performing incident analysis include lack of detailed information about the architecture of the cloud relevant to an incident, lack of information about relevant event and data sources held by the cloud provider, ill-defined or vague incident handling responsibilities stipulated for the cloud provider, and limited capabilities for gathering and preserving pertinent data sources as evidence. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought.

General Recommendations:

A number of significant security and privacy issues were covered in the previous subsections. Table 1 summarizes those issues and related recommendations for organizations to follow when planning, reviewing, negotiating, or initiating a public cloud service outsourcing arrangement.

Table 1: Security and Privacy Issue Areas and Recommendations

Areas	Recommendations
Governance	• Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. • Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
Compliance	• Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements. • Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. • Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.
Trust	• Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. • Establish clear, exclusive ownership rights over data. • Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system. • Continuously monitor the security state of the information system to support on-going risk management decisions.
Architecture	• Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
Identity and Access Management	• Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.
Software Isolation	• Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.
Data Protection	• Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data.

	• Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value. • Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.
Availability	• Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements. • Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.
Incident Response	• Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization. • Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. • Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

G.4 Mobile Appendix

Mobile Appendix

Introduction

Mobile devices present a unique security challenge with regard to the correct application of CJIS Security Policy requirements. This appendix is intended to provide best practices based on industry standards and on methods to achieve policy compliance in mobile device employment scenarios. The technical methods used to achieve compliance with CJIS Security Policy will typically be different within the mobile environment than those used in fixed locations. Many of the security features and capabilities inherited by endpoint devices from the fixed environment are either not present or present in a different form in the mobile environment. Additionally, the basic technologies used in some types of mobile devices may adequately fulfill some of the CJIS Security Policy requirements which would require additional software or added features in a traditional fixed computing environment. Due to the complexity and rapid evolution of the mobile environment, this Appendix will remain as device and vendor agnostic as practical, however certain key requirements for specific mobile operating systems will be identified for the major mobile operating systems (e.g. Apple iOS, Android) as the underlying technologies are fundamentally different and offer different levels of built-in compliance to CJIS Security Policy.

Sections within this appendix will provide recommendations regarding priorities and level of effort versus value of applying certain security controls in the mobile environment. These recommendations do not supersede or modify the requirements listed in the CJIS Security Policy, and are intended to describe the effect of inherent security functions and inherent device limitations in many mobile platforms that impact the application of policy elements in the mobile environment.

Mobile Device Risk Scenarios

There are multiple risk scenarios that may apply to mobile devices depending on the category of device (e.g. Laptop, Tablet, and 'Pocket sized' devices such as smartphones) and the methods of device connectivity (e.g. cellular service, WiFi + Cellular, WiFi only). Device category and method of connection define the technology types within the device which inherently affects the total level of compliance with CJIS Security Policy that can be obtained by the mobile device.

It is advisable for acquiring agencies to review the mobile device guidance in this Appendix prior to completing selection and acquisition of particular devices. Both the device category and connectivity methods installed and configured on the device will impact the overall risk scenario associated with the device and may significantly affect the effective cost to bring use of the device in compliance with the CJIS Security Policy. For instance, inclusion of cellular radios with the ability to remotely control a device significantly changes the risk scenario by allowing remote tracking, file deletion, and device management which could provide a higher level of CJIS Security Policy compliance than a WiFi only device that does not guarantee the ability to remotely manage the device. However, inclusion of cellular technology may significantly increase the initial device costs and incur ongoing subscription costs. Appropriate choices based on the intended use of the device along with the types and methods of Criminal Justice Information (CJI) data to be accessed could greatly reduce agency cost and enhance security.

Device Categories

This appendix defines risk levels for three categories of devices. Prior to reading individual sections of this Appendix, the agency should identify which device categories will apply to their employment scenario. If multiple categories of devices are employed, individual technical configurations and local policy will likely need to be defined for each category of device based on the risk inherent in the technical characteristics associated with each device category.

Laptop devices

The laptop device category includes mobile devices in a larger format that are transported either in a vehicle mount or a carrying case and include a monitor with attached keyboard. This includes all traditional laptop computers that utilize a 'traditional', full featured operating system (e.g. Windows or a Linux variant). Also included in this category are 'tablet' type full featured computers running a traditional full featured operating system but without an attached keyboard. The main defining factor is the use of a full featured operating system and a form factor too large to be carried in a pocket. In general, devices of this type connect via WiFi only, but may include an internal cellular access card in some cases.

The risks associated with this device type are similar to a standard desktop computer at the technical level, but are increased due to the potential to connect directly to the internet without the benefit of organizational network security layers (e.g. network firewall, IDS/IPS, network monitoring devices). There is also an increased risk of intentional device theft from vehicles or unsecure locations as these devices are too large to be carried on the authorized user's body. There may be increased risk from the limited technical ability to wipe or track a lost/stolen device depending on the particular technical means used for remote device connectivity (e.g. cellular or WiFi).

In general, the technical configurations for compliance with most of the CJIS Security Policy that is accomplished via the operating system (e.g. auditing, access control, etc) will remain consistent with normal fixed location computing systems for laptop devices, but some functions may operate in an unexpected manner due to lack of constant connectivity. Thorough testing of applied security policy elements within the expected mobile environments will help ensure the applied policy configurations remain effective and appropriate when applied to mobile laptop devices.

NOTE: Some newer devices running multi-function operating systems (e.g. Windows 8 or similar multi-mode operating systems) may exhibit technical features associated with both laptop and tablet device categories based on their current operating mode which may be reconfigured by the user on demand. If this is the case, it will be necessary to assess and configure multiple operating modes to be compliant with CJIS Security Policy on the device, or restrict the operating mode to one category of operation.

Tablet devices

The tablet device category includes larger format devices transported via vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard. These devices utilize a limited feature operating system (e.g. Apple iOS, Google Android, Windows mobile) that is inherently more resistant than a traditional operating system to certain types of network based technical attacks due to the limited feature sets. Additionally, limited functionality operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers. This inherently limits the types of services that can

function effectively on the devices (e.g. traditional real-time anti-virus software) as the base operating system may not be designed to allow installed applications enhanced execution priority in the background and or the ability to examine the contents or communications associated within another application. However, this same design methodology significantly limits the vectors available for malware transmission and the device or application data actually accessible to malware if a device becomes infected.

Tablet devices will have different risks associated depending on the installed and configured methods for network access (e.g. ‘always on cellular’ vs. WiFi only). Physical risks associated with this category are similar to the laptop category for enhanced likelihood of intentional theft or device hijacking while unattended, while the technical risks are similar to the pocket device category.

Pocket devices/Handheld devices

The pocket/handheld device category is technically similar or identical to the tablet category and is primarily differentiated by device form factor. Pocket/handheld devices are characterized as having a limited functionality operating system and a small form factor intended for carry in a pocket or ‘holster’ attached to the body. The bulk of this category will be cellular ‘smartphones’ with integrated cellular data connectivity, however devices intended to be worn or carried on the body (e.g. portable fingerprint devices) may also be included in this category if they operate using a limited functionality operating system. Custom or specialty devices may meet the form factor distinction for this category, but operate using a full feature operating system. In rare cases of this nature the employing agency should apply security guidance and principles in this appendix for both the laptop and pocket device categories.

Risks associated with this category are a reduced threat of theft to a stored devices (e.g. device left unattended in a vehicle) since these devices are typically carried continuously by the authorized user, but include a greater risk of temporary or permanent loss of control due to the device being misplaced by the authorized user.

Due to the installation of a limited functionality operating system, the technical threat to these devices via a network based attack is significantly lower than the laptop category, however, the threat of unauthorized access at the device level may be higher if the device is lost due to technical limits on multi-factor authentication to the operating system itself and practical limits to device passwords due to screen/software keyboard limitations.

NOTE: Data accessible on pocket or tablet devices simply through the entry of a single device PIN or password should not be considered secure due to the likelihood of enhanced password guessing based on fingerprints/smudges on the device touch screen. Any data stored on devices of these types should be protected within a separate secure container using Advanced Authentication.

Device Connectivity

There are three main categories of device connectivity that are associated with varying risk levels and threats to the devices. The Three categories are: Cellular Network Only (always on), WiFi Only (includes ‘on demand’ cellular), and Cellular (always on) + WiFi network. The risks associated with connectivity categories are general risks and may apply differently to any particular device at different points in its usage or lifecycle. Particular device configurations either through the operating system or a third-party mobile device management (MDM) system may be

able to significantly control and define which particular connectivity risks may be associated with a particular device.

Cellular Network Only (always on)

Cellular network connectivity is characterized by ‘always on’ network connection through the device internal radio to a cellular network provider. There is a reasonable assurance that devices with ‘always on’ cellular can be tracked, managed, or wiped remotely if lost or stolen. This will significantly reduce risks associated with loss of the device and attempted illicit access to the device. One important consideration for this risk category is characterization of the device as ‘always on’ or ‘on demand’. In effect the difference is typically a configuration setting, which in some cases may be changeable by the user. In particular most cellular smart phones contain ‘airplane’ mode settings that disable all internal radios allowing a user authenticated to the device operating system via password or personal identification number (PIN) to disable the cellular system. Access to this functionality may be disabled through the use of some MDM systems which would necessitate a complete power down of the device while carried on aircraft. Additionally, someone illicitly obtaining a device with properly configured password requirements and screen lock timeouts would be unlikely to guess the device password before the device was reported stolen in order for them to disable the cellular connection and prevent tracking or a remote wipe of the device.

Cellular networks do not allow for the same level of exposure of individual devices to random access from the internet. This significantly reduces the potential network based attack vectors that might reach a cellular connected device. The risk scenario in most cases from a network based attack would be similar to a device protected behind rudimentary network defenses (e.g. standard firewall but NOT advanced intrusion detection/prevention) Cellular device communications cannot typically be accessed by other ‘eavesdropping’ devices physically close to them without significant specialized equipment and can be considered well protected against network attacks below the nation/state level of technical capability by the hosting technical infrastructure and technology inherent in the device. However, network based attacks that utilize connections initiated by the user device may still succeed over the cellular infrastructure. For this reason, the technical protections inherent in the cellular infrastructure provide limited protection against user/device initiated actions (e.g. web surfing on a cellular connected web browser). Therefore, the protections provided by always on cellular connections are primarily in the ability to remotely access the mobile device for tracking or data deletion in case of device loss or compromise, which combined with a limited functionality device operating system, the protections are generally equivalent to a ‘personal firewall’ if properly configured and supported by a well-designed organizational infrastructure. However, that equivalency does not apply to full featured operating systems connected through cellular infrastructure.

NOTE: It should be noted that a technically capable, intentional, thief knowingly obtaining an ‘always on’ cellular device for the purpose of data theft can physically disable the radio by utilizing a Faraday cage or similar external electromagnetic shield device while attempting to guess the device password. While technically possible these methods require specialized equipment and high technical expertise and would be very unlikely to be employed except for specifically targeted attacks. When always on cellular connectivity is combined with a robust incident reporting process and user training for rapid response to device loss or theft, the associated risks can be minimized.

WiFi only (includes ‘on-demand’ cellular)

WiFi only devices do not include cellular radios or include cellular radio that must be manually activated or ‘connected’ to the cellular network. They connect to the network or internet through WiFi ‘hotspots’ or external access points or manually to cellular networks. Some MDM or device configurations may be able to limit the types and specific WiFi access points the device can connect to, which may change the risk scenario of the device to a similar risk scenario as the Cellular Network Only scenario. However, if mobile devices are permitted (through technical and or policy decisions) to connect to any WiFi access point designated by the device user, the overall device risk scenario is high and the device may be accessible to a large number of potential network based attack vectors. Unrestricted WiFi access is not recommended on any agency owned device, but must be assumed to exist on any personally owned device authorized to access CJI. Significant compensating controls may be needed to ensure devices accessing CJI over ‘public’ WiFi access points are not susceptible to communications network eavesdropping, credential hijacking or any of the various potential man-in-the-middle attacks possible through access point spoofing. The communications security risks can be significantly mitigated by mandatory device configurations (e.g. MDM based policy) that only allow devices to connect to cryptographically verified agency controlled WiFi access points.

WiFi only or devices with ‘on-demand’ cellular access (e.g. user or event driven cellular access initiated from the device and not from a centralized management location) are significantly more at risk from data loss subsequent to device loss or theft as there is no guarantee the tracking or remote wipe can be initiated once the device is out of agency control. This can be mitigated by utilizing tracking/anti-theft products that require a periodic network connection to authorize access and perform automated device locking (‘bricking’) or remote wipe if network connections are not made within a specified period. Software of this nature is generally available for full featured laptops but may not be available for limited feature mobile operating systems.

Cellular (always on) + WiFi Network

This is a hybrid scenario that has become typical with most ‘smartphones’. These devices contain both the always on cellular connection, but may also be configured to access local WiFi networks for enhanced bandwidth. In considering devices with these technical characteristics, the theft/loss risks are similar to the cellular only scenario (due to tracking and remote access through the cellular connection), while the data and network based risks must be considered to be similar to the WiFi scenario unless the capability of the device to connect to WiFi networks is limited by technology or policy to agency owned WiFi Access Points configured in accordance with the CJIS Security Policy. Careful consideration must be made to the particular configurations, management systems, and human oriented operational policies based on the particular technical capabilities and configurations of these types of devices.

Incident Handling (CJIS Security Policy Section 5.3)

Additional or enhanced incident reporting and handling procedures will need to be developed to cover mobile device operating scenarios. Various exploits and methods to compromise mobile devices require either specialized equipment or lengthy operations to implement. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. However, parallel or special incident handling procedures with associated equipment or systems may need to be put in place to properly respond to incidents involving mobile devices. This section lists three areas where enhanced incident handling and

response processes may need to be implemented to ensure mobile device compliance to the incident handling policy in Section 5.3.

If personally owned devices are utilized within the environment in a Bring Your Own device (BYOD) scenario, specialized and costly incident handling procedures and processes may need to be developed to support compliance for those devices. The costs associated with enhanced incident handling procedures may need to be incorporated in the cost and risk based analysis to allow personally owned devices in the BYOD scenario, as the technical methods and risk to achieve compliance under BYOD scenarios may exceed any cost savings potentially achieved through BYOD.

Loss of device Control

Mobile device users should be trained and provided with explicit user actions in case positive control of a mobile device is lost for any period of time. Loss of positive control means the device is in the physical control of non-CJIS authorized individual or the device is left unattended in an unsecure location (e.g. counter of the coffee shop). Even if the device is recovered quickly there is significant risk that either the device settings could be tampered with or data on the device could be illicitly accessed. The level of detail and particular scenarios identified in the agency incident response plan should be consistent with the presence of persistent CJI on the device or the technical means used to access CJI from the device (e.g. ask the question: “Is it reasonable to assume CJI could be accessed”) as well as the degree of device configuration control exercised by the user from the device main login. At a minimum, special incident handling procedures should be developed for the following scenarios:

- Device known to be locked, control loss of minimal duration
- Device lock state unknown at time of control loss, duration of loss minimal
- Device lock state unknown at time of control loss, duration of loss extended
- Device known to be unlocked at time of control loss, duration of loss more than momentary.

NOTE: Organizations should define appropriate time value criteria based on the operational environment for the above scenarios. For instance, a ‘momentary’ loss of control might be considered a matter of seconds in a situation where no one could reasonably have accessed the device, while ‘minimal’ durations might include a few minutes of time and ‘extended’ periods would be any time longer than a few minutes.

Other scenarios should be addressed as appropriate to the intended device employment, with explicit user and organizational actions identified based on the device technologies and any organizational management capabilities.

Total Loss of device

Incident response scenarios for the total loss of the device should be developed based on the methods/storage of CJI on the device, the lock state of the device at time of loss (known locked, known unlocked, or unknown), and the technical methods available for remote tracking or wiping of the device. It is critical to implement incident handling procedures quickly in this case. Remote wipe functions can be implemented for always on cellular devices with a high potential for success that may include positive confirmation from the device that the wipe was completed. However, for WiFi only and on demand cellular devices, incident handling procedures that lock the device out

of accessing CJI may be necessary, while there would be no guarantee that any CJI stored on the device could not eventually be accessed. For this reason, CJI should not generally be stored directly on WiFi only or on-demand cellular devices unless an extremely robust anti-tamper system is in place on the device itself.

Potential device Compromise (software/application)

Incident response scenarios for potential device compromise through intentional or unintentional user action should be developed to ensure compliance with policy. This includes rooting, jailbreaking or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from either intentional threat agent actions or accidental user actions). Triggers for this incident handling process may be driven from either user notification or electronic detection of device tampering from an audit or MDM compliance check.

Audit and Accountability (CJIS Security Policy Section 5.4)

The ability to implement some Audit and Accountability functions specified in the CJIS Security Policy on mobile devices with limited function operating systems (e.g. Android, Apple iOS) is not natively included within the operating system. Either additional device management systems, enterprise mobility management (EMM) or MDM, or auditing from systems accessed by the mobile device will be necessary to ensure appropriate levels of auditing exist.

Auditable Events (reference 5.4.1)

Some of the specific audit requirements in the CJIS Security Policy may not be technically relevant to the mobile operating system due to its internal functioning. To achieve compliance with the CJIS Security Policy it will be necessary in most cases to utilize some form of MDM or EMM system. Additional auditable events that compensate for the technical limitations of limited function mobile operating systems may be available through the use of MDM systems (e.g. association of event with global positioning system (GPS) location of the device). Specific auditable events of interest in the mobile environment will depend on the intended device usage, compartmentalization of data on the device, and options available with the specific technologies employed. For instance, item 2 in Section 5.4.1.1 indicates an auditable event includes attempts to modify elements of user account modification. Due to the limited internal functions of mobile operating systems, this event type is not relevant to the operating system itself as they are generally provisioned with only a single non-modifiable user account on the device. To achieve compliance in a scenario where CJI is stored or accessed from a secure application on the device, auditing of access to the secure application either through application design, or third party MDM capability may provide an acceptable compensating control. For compliance with the policy each auditable event and event content must be compared to the particular technologies and applications employed to determine if adequate compensating controls are being met for audit items that either do not apply to mobile technologies or cannot be implemented within the technology itself.

Alternative and compensating controls that provide detailed audit of access to CJI either on the mobile device itself or through a controlled application to a central server may provide equivalent auditing capability to the events specified in the policy. However, multiple auditing systems may be required to replicate the auditing provided at the operating system level by a full function operating system. Therefore, the overall auditing design should take into account retrieval and

consolidation of events or audit data from multiple auditing systems as appropriate to comply with policy.

Audit Event Collection

Mobile devices without an ‘always-on’ cellular connection may pose technical challenges to ensure any audit records collected and stored on the mobile device itself can be retrieved for review and analysis per the CJIS Security Policy. Alternatively systems which explicitly require a network connection to a central server to access data or decrypt on-device storage may provide acceptable audit event collection and reporting since there is a guarantee that network connections must be in place for CJI to be accessed. Careful consideration should be made regarding the accessibility of audit records when developing the mobile audit scheme.

Access Control (CJIS Policy Section 5.5)

Access control associated to limited functionality mobile operating systems will typically operate in a different manner than full function operating systems. For instance there is normally not a provision for multiple user accounts on many mobile operating systems which may mean the policy requirements for access control (e.g. regarding account management) would not be apply to the mobile operating system, but should rather be applied to a particular application, either stand-alone to the device or as part of a client server architecture. Application of access control policy identified in the CJIS Security Policy will often need to be applied to elements of the total system beyond the device operating system.

For example, CJI stored or accessed from a secure mobile application that requires connectivity to a CJIS authorized server architecture could potentially accomplish most or all of the access control policy elements based on user authorization via the secured application and be largely independent of the mobile operating system. Alternatively, if storing CJI in ‘general’ purpose data storage containers on a mobile device it may not be possible to achieve compliance with the CJIS Security Policy. Careful consideration and deliberate design of mobile applications or data storage will be required to achieve compliance on mobile devices.

Due to the inherent nature of limited function mobile operating systems, very tight access controls to specific data is actually implemented within the operating system. This effectively prevents applications from accessing or manipulating data associated with other applications to a very high degree of confidence as long as the device is not rooted or jailbroken. However, the device user is automatically granted access to all device data through the associated application unless the application itself has a secondary authentication and access control methodology. Additionally, since basic device functions (e.g. phone) are typically protected using the same password or PIN as the device level encryption, use of a weak PIN to allow easy access to basic device functions largely negates the value of the integrated device encryption.

If personally owned devices are utilized within the environment (BYOD scenario), specialized and costly access control methods may be required to reach compliance with CJIS Security Policy. The costs associated with enhanced access control procedures and technologies should be incorporated in the cost and risk based analysis to determine whether or not to allow personally BYOD, as the technical methods and compensating controls required for CJIS Security Policy compliance are likely to exceed any potential cost savings for implementing BYOD.

Device Control levels and access.

Limited function mobile operating systems are typically very constrained on the levels of access provided to the user. However, intentional user actions (e.g. installing an application and accepting inappropriate security access levels for that application) may bypass some of the built in security protections inherent in the limited functionality devices. Compliance with CJIS Security Policy may be difficult without the addition of strict device control policy. In a mixed environment (e.g. agency owned devices and BYOD), access control policy with BYOD systems may be impractical or impossible to fully implement.

Embedded passwords/login tied to device PIN.

Limited function mobile operating systems typically allow the association of multiple passwords and access credentials with particular applications. The system access provided by these embedded credentials will often be tied to the device password or PIN. An example would be access to device integrated email and calendar applications. Alternatively a 'corporate' email application may independently encrypt the data associated with the application and required a separate login from the device itself. Access to CJI utilizing only the device level password or PIN and device embedded credentials is not compliant with CJIS Security Policy unless protected with Advanced Authentication, which is not currently possible on most devices. Therefore, use of integrated device functions (e.g. built in email or chat) to store or transmit CJI would also not be compliant.

Access requirement specification

In general, due to weaknesses associated with password guessing based on analysis of fingerprints or swipes on the device touch screen, short (4-8 digit) device PIN numbers provide limited security to a determined password guessing attack. Conversely, utilization of a robust password at the device level may be inconsistent with quick access to basic device functions (e.g. phone). When developing specific CJIS compliant access control and authentication schemas a layered approach with the device PIN protecting only the basic device functions (e.g. phone, camera, non-secure applications) and a more robust password or multifactor authentication used to protect applications or data storage may achieve policy compliance where the device password/PIN would not. In a layered security deployment, careful attention must be placed on the capability to share data (e.g. cut and paste or screenshot functions) between secure applications with CJI or CJI access and basic device functions with limited security controls.

Special Login attempt limit

Depending on the access and authentication scheme applied to the mobile device, it may be appropriate to fully comply with the CJIS login attempt limits within a secure application or container and not solely at the device level. However, the device itself should have login attempt limits consistent with the risk associated to the data or configurations accessible on the device itself. Since mobile devices are inherently portable, and can easily be removed from a location. Brute force attempts to gain access to the system, especially when protected only by a short PIN, are likely to be successful given sufficient time. Special consideration should be made based on device connectivity methods (cellular, WiFi, etc) on the appropriate number of unsuccessful login attempts that will be allowed and the resultant actions taken by the device. Most devices either natively allow for the device to wipe itself after a failed number of attempts, or allow the application of EMM/MDM applications to perform wiping actions after a predetermined number of failed login attempts.

Login failure actions

Mobile devices with or without MDM software can typically be configured to perform actions based on serial unsuccessful login attempts. Appropriate actions to configure may be dependent on the data resident on the device and the connectivity method employed by the device. Most devices can be configured to delete all data on the device and/or issue an alert to the network if a number of incorrect passwords are entered. This is a very advantageous feature, however specific configuration of the number of attempts and resultant action must be considered against the state of the device after an unsuccessful attempt action is triggered. A full device wipe will typically leave the device in a fully or partially non-functional state which could introduce risk if part of the intended use is time critical phone calls. Where possible, full device wipe associated with unsuccessful attempts at the device level password should be configured but the number of invalid attempts may exceed the CJIS Security Policy at the device level if all CJI on the device is protected by an additional layer of encryption protected by a subsequent secure application authentication method that is technically prevented (via complexity rules or entry rules) from being the same as the device level authentication and the secure application is configured in accordance with the policy and also contains a secure data wipe capability after a specified number of incorrect authentication attempts.

System use Notification (CJIS Policy reference 5.5.4)

Agency policy should include specific mandatory language consistent with the CJIS Security Policy to identify the device restrictions and consent. However, due to screen size limits, some mobile devices may not be technically capable of displaying the full text used with traditional operating systems. To achieve compliance agencies should contact their legal department for appropriate wording of a short version of the system use notification that can be set to display within the constraints of the device lock screen. This may be accomplished through embedding the text into an image displayed on the lock screen or some other external device labeling method if the device does not permit sufficient text to be displayed.

In a BYOD environment or mixed (agency owned and BYOD), it may be necessary to develop or deploy custom applications that can achieve compliance with the system use notification upon access and prior to any CJI access being allowed.

Session Lock (CJIS Policy reference 5.5.5)

Due to the portable nature of mobile devices the session lock limit in the general CJIS Security Policy may be excessive in the mobile environment for certain device functions and insufficient for other functions based on intended device usage. Agencies should examine the minimum lock time practical for all mobile devices based on their employment scenario and ease for which a user can manually lock the device. The actual session lock times should be adjusted as appropriate to the device type, device operational location, and the data accessible on the device when unlocked. Pocket size devices are at greatest risk if screen lock times are insufficient, however, for devices used in emergency response or communication, extended lock times at the basic device level may be considered if CJI is subsequently protected by an application or web interface utilizing more stringent secure locking functions. A well designed solution may include multiple session lock settings at the device and individual application levels to ensure the CJIS Security Policy requirements are met for CJI access, while other device functions are accessible under different session lock configurations.

Device WiFi Policy

Specific WiFi configuration policy should be developed based on the intended use environment and data access requirements for the device. The policy should explicitly cover configuration of device connections. Technical methods specific to the mobile technologies may need to be implemented to ensure all mobile devices are compliant with CJIS Security Policy. Current CJIS Security Policy provides detailed configuration requirements for WiFi connections, however it was originally intended for defining requirements for fixed infrastructure WiFi (802.11) supporting wireless within a facility. The security requirements identified for fixed infrastructure installations are applicable to mobile usage, however there are several mobile specific scenarios where the requirements may not be clear. The following sections identify areas not specifically covered in the existing policy that will require special handling to ensure wireless connections are compliant.

Hotspot capability

Many mobile devices now include the capability to activate an internal WiFi hotspot that allows other devices to connect through the hosting device to the internet over the devices cellular radio. While this is a potentially valuable capability when multiple law enforcement devices may need localized internet or network access, mobile hotspots should be configured as consistent with the CJIS Security Policy on wireless access points. Connections must only be accepted from known and approved devices in order to protect the integrity of the hosting device as well as the communications security of other connected devices. Since most mobile hotspots are not technically capable of providing the device authentication required for infrastructure wireless, use of mobile hotspot capability should assume the overall portable WiFi network itself is not secure and CJI should not be transmitted or exposed on the network without appropriate encryption.

Connection to public hotspots

There are significant risks to connecting to public wireless access points. Rogue access points masquerading as legitimate public access points may allow for man-in-the-middle, eavesdropping, and session hijacking attacks. While not specifically prohibited in the current CJIS Security Policy, it is recommended that connection to public internet access points be technically restricted by device configuration or MDM systems if possible. CJI access mechanisms from mobile devices should include robust authentication methods specifically designed to prevent interception or hijacking of CJI or user information through the use of a rogue access point masquerading as a legitimate public wireless access point. Transmission encryption alone may not provide sufficient protections when device connections originate at public hotspots. Since the public hotspot controls access to all network services at the connection point (e.g. Domain Name System) attacks against the transmission path are possible that would not normally be feasible in a fixed environment where communications exist between two secured network enclaves.

Cellular Service abroad

If mobile devices are used outside of the United States, especially if connected to foreign cellular networks, specific handling procedures may need to be developed for the use of the device while abroad and the assessment or configuration check of the device state once the devices are returned to the United States. Certain device internal functions on cellular devices may be modified or compromised by the cellular carrier as the devices are intended to have certain parameters configured by the cellular service provider which is considered a 'trusted' entity by the device.

Cellular carriers within the United States are constrained by United States laws regarding acceptable modifications to devices. Similar legal constraints cannot be assumed to exist in some areas of the world where laws and regulations for data and personal privacy may allow cellular carriers significantly more leeway in changes made to devices on their networks.

Security plans involving cellular connected devices that will be connected to foreign cellular networks should include technical and policy controls to ensure device use while abroad, data resident on the device while abroad, and the software integrity of the device once returned to the United States are all appropriate to the specific device and threat levels associated with the expected foreign travel. This should explicitly include considerations for devices in which an internal subscriber identity module (SIM) card is inserted into the device to obtain Global System for Mobile (GSM) cellular connections abroad to ensure any residual data on the SIM card is properly purged. Additionally, incident handling procedures may need to specify more stringent responses to even momentary loss of device control, and it may not be possible to assume tracking, anti-theft, and remote data wipe functions that work in the United States would be functional in all potentially visited geographic and political regions.

Bluetooth

Mobile devices utilizing Bluetooth should be evaluated for their ability to comply with the CJIS Security Policy Bluetooth requirements prior to acquisition. This includes the data device itself and any authorized Bluetooth accessories which will be associated to the device. While the technical security in current versions of Bluetooth is significantly stronger than legacy versions, mis-configuration of devices can still pose a significant threat in the mobile environment. If not specifically utilized for a required purpose, it would likely be most cost effective to disable or restrict the device Bluetooth radio utilizing device configurations or an MDM product. Additionally, the using agency may need to develop technically extensive training or user awareness programs to ensure use of Bluetooth capability does not render the device out of compliance if device users have the ability to make Bluetooth associations to the device. Specific instructions or guidance for specific devices could be developed to ensure all implementations are compliant.

Voice/Voice over IP (VoIP)

Cellular voice transmissions are distinctly different at the technical level than Voice over IP (VoIP) transmissions using voice/video applications (e.g. FaceTime, Skype). The use of VoIP is not specifically granted the exemption identified in CJIS Security Policy Section 5.5.7.3.2. Agencies wishing to use capability of this type should ensure the specific technical implementation complies with the Policy on authentication and data encryption.

Chat/Text

Device integrated chat/texting applications and many common third party chat applications authenticate and are identified using embedded passwords or the device identifier only. These functions should not be considered secure or appropriate for transmission of CJI data. Texting functions that utilize a cellular service providers Short Message Service (SMS) or Multimedia Messaging Services (MMS) functions do not constitute a secure transmission medium. Third party applications utilizing appropriate encryption and authentication methods independent of the device password/PIN may provide a compliant solution where the device integrated utilities are will not provide a compliant solution.

Administrative Access

Local administrative access to the mobile device, regardless of device category should be restricted by some mechanism. For traditional operating systems, configuration of a separate administrative account other than that used for normal logins to the device is an acceptable method to ensure appropriate access permissions to the mobile user for which they are authorized. However for limited functionality mobile operating systems (e.g. Android, Apple iOS) internal permissions and accounts assume a single authorized device user with explicitly defined permissions. Those permissions may be modified through policy applied to the device, but are typically global to the device itself. As a result, to ensure appropriate separation of access permissions, it may be required to ensure specific applications or software on the device are configured with individual authentication methods to separate application data from ‘general user’ access. Without additional authentication at the application level, access to specific application data would be available to any user with the ability to unlock the device. This may be appropriate in some scenarios with a high degree of assurance that the device can only be accessed by a single user, but sufficiently stringent device passwords and short screen lock times may prove problematic for practical use of some device functions. An alternate method to ensure strict separation of ‘routine’ device functions which may be accessed by multiple individuals (e.g. phone function if loaned to someone for a critical call) is to ensure any method used to access or store CJI has a separate and more stringent authentication method configured with rules that make it impossible to use the same authentication credential (e.g. PIN/Password) on both the device authentication and the application or function with access to CJI.

Rooting/Jailbreaking

‘Rooting’ (Android OS) or ‘Jailbreaking’ (Apple iOS) refer to intentional modifications to the mobile device operating system in order to grant the device user or an installed application elevated control that would not normally exist on the device. The security model internal to the various mobile device architectures vary significantly, however the common effect of rooting or jailbreaking the devices is to bypass many or all of the built in security features. The security feature bypass may be universal to all device features and installed applications once completed. Intentionally rooting or jailbreaking mobile devices should be avoided in any scenario as it potentially defeats all built-in data access and segregation controls on the device. Additionally the rooting or jailbreaking process itself has a heightened risk of introducing malicious code as part of the process, and also substantially increases the risk for malware to infect the device through user action. Extreme caution should be used if software is being installed that requires the devices to be rooted or jailbroken for the software or application to function. This is inclusive of purported security software that requires a rooted or jailbroken device to function. For example, on both the Android and Apple iOS platforms, the built-in security features for data access and memory segmentation prevent the effective operation of ‘traditional’ anti-virus and intrusion detection/prevention software. Software or applications purporting to perform these functions but requiring rooting or jailbreaking of the device and may actually accomplish the anti-virus or IDS/IPS function but are also likely to significantly increase the overall risk associated to the device by effectively disabling most or all of the integrated security features. A careful risk-based assessment should be conducted by a trained security professional prior to allowing the operation of any rooted or jailbroken mobile devices regardless of intended use. Significant compensating controls would be required to return a rooted or jailbroken device to minimal compliance with most of the CJIS Security Policy and would likely not be a cost effective approach.

NOTE: There is a distinction between rooting a ‘stock’ Android installation vice the installation of a separately supported secure operating system. There are secure versions of Android available or that can be developed based on the open source Android source code and compiled for installation on a particular hardware device. Installation of a secure, supported mobile operating system that replaces the device original operating system may significantly enhance the security of the device and should not be confused with ‘rooting’ and Android installation. Due to the close integration of operating system security with hardware elements, and the proprietary nature of Apple source code, there are not currently separate ‘secure’ versions of the Apple iOS and it is unlikely they will be developed.

Identity and Authentication

Due to the technical methods used for identity and authentication on many limited functionality mobile operating systems, achieving compliance to CJIS Security Policy may require layering of identification and authentication mechanisms. With the complexity and large number of potential identity and authentication solutions in the mobile environment emphasis must be placed on designing secure identity management and authentication architecture prior to the selection of individual devices or applications. Failure to consider a robust identity and authentication scheme as part of system design or acquisition will significantly increase the risk of subsequent noncompliance with CJIS Security Policy and potential added costs for a remedial solution. Many identity and authentication schemes used by existing commercial applications may make claims that appear to be consistent with CJIS Security Policy Advanced Authentication requirements, however, extreme care must be taken to ensure the actual technical implementation is compliant with policy.

Utilizing Unique device Identification

Some commercial applications and features integrated with some mobile operating systems permit the mobile device to be uniquely identified in a cryptographically robust manner. Any authentication schema that considers the possession of the mobile device as a factor in uniquely identifying and authenticating a CJIS authorized user must also include factors beyond than mere possession of the device. Larger form factor devices that cannot be carried on the person of the authorized user should not rely on possession of the device as an identifying factor, but may still include identifying capability within the device to provide assurance that the device itself is an authorized device. This should still be coupled with multi-factor advanced authentication to the device itself or the application hosting CJI. Coupling unique device authentication with robust advanced authentication of the user provides a high degree of confidence that both the specific device and the operator of the device are correctly identified. Utilizing device unique identification in order to authorize initial connections from the remote device back to the CJI hosting system or enclave provides additional protection to the CJI hosting system to reduce the attack surface of the hosting system and should be considered a good practice, but not in itself an authentication mechanism for the device user.

Certificate Use

One method for uniquely identifying mobile devices is to place part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of identification or authentication in a larger scheme, a certificate alone placed on the device should not be considered valid proof that the device is being operated by an authorized CJIS user, only that the device itself is authorized to host CJIS users. Additional user identification and authentication should be used to supplement any device certificate installed. Using a PIN or password separate from the device login to ‘unlock’ the certificate from cryptographic storage within a secure application will provide an additional layer of security and may increase the confidence level the device is being used by the intended user. However, use of public/private key pairs or pre-shared encryption keys can be utilized as part of an architecture to protect against certain session hijacking or man-in-the-middle attacks a mobile device may be susceptible to if connected to public internet connections.

Certificate Protections

Any certificates or cryptographic keys stored on any mobile device should include protections against the certificate or key being extracted from the device. Additionally certificates or other keys stored on mobile devices that grant the device special access or unique identification should be configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts. Alternatively, methods may be used to revoke or invalidate the unique certificate or keys associated with a device.

Minimum Password/Pin (Reference CJIS Security Policy Section 5.6.2.1)

The minimum password protections identified in the CJIS Security Policy may not be appropriate for the device PIN/password due to immediate access requirement for some device functions (e.g. phone function) secured by the device PIN/password and the difficulty to enter a complex password under emergency conditions on a small screen. In cases where the risk of a complex password on the device itself is deemed significant, a layered authentication approach may be necessary where CJI or access to CJI is protected via one or more additional layers of access control beyond the device PIN/password. In cases where the CJI or access to the CJI is cryptographically segregated from applications accessible using the device level PIN/Password (e.g. secure application or secure browser vice the built-in browser) the authentication mechanism for the secure application or browser may satisfy the CJIS Security Policy requirements if fully compliant as a stand-alone application.

Configuration Management

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of traditional full featured operating systems may not function properly on limited function mobile operating systems. Configuration Management systems in the mobile environment may be designed in order to duplicate some of the functions typically performed by traditional anti-malware systems that will not function properly on some mobile operating systems.

Mobile Device Management (MDM)/Enterprise Mobility Management (EMM)

MDM and EMM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented. MDM capabilities include the application of mandatory policy settings on the device, detection of

unauthorized configurations or software/applications, detection of rooting/jailbreaking of the device, and many other security policy related functions. In many cases, the most cost effective way to achieve CJIS Security Policy compliance on mobile devices is the selection of MDM or EMM applications and infrastructure appropriate to the mobile operating systems and intended access to CJI on the mobile devices. MDM/EMM functions may be applicable to most of the CJIS Security Policy requirements and allow for significant compensating controls in areas where traditional methods of CJIS Security Policy compliance are not technically feasible. Section 5.5.7.3.3 of the CJIS Security Policy specifies the minimum functions required for MDM. However, careful selection of the MDM product will potentially provide a cost effective method for additional areas of compliance in the access, auditing, incident response, authentication, media protection and system integrity sections of the CJIS Security Policy.

Device Backups/Images

Device images and backups provide protection against data loss, but also provide a method to quickly recover a device after damage or potential compromise. Due to an inherently limited ability to access the internal file structure of mobile devices, it can be difficult to easily identify a device compromise or illicit modification of the device. Some device imaging and assessment software may provide a secondary forensic capability, especially if there is intent for the device to be used outside the United States.

Bring Your Own device (BYOD) employment

BYOD environments pose significant challenges to the management of secure device configurations. In many cases it may be impossible to apply effective security that is acceptable to the device owner or it may require extremely costly compensating controls to allow access to CJI on personally owned devices. While allowed by the CJIS Security Policy, agencies are advised to conduct a detailed cost analysis of the ancillary costs of compliance with CJIS Security Policy on personally owned devices when they are approved for use. In some cases, a BYOD user may agree to abide by the same device configurations and limitations as imposed on an agency owned device, but signed user agreements should still be in place to ensure the agency has a legal right to recover or clear the device of all data prior to device disposal or employee termination. In other cases, robust secure applications may provide acceptable levels of compliance in a BYOD environment for limited CJI access but application design and architecture should assume the device itself is un-trusted. If MDM/EMM software capable of detecting rooting or jailbreaking of the device is not installed, any CJIS or data access occurring from the device is at a substantially higher risk of compromise.

Configurations and tests

Common configurations specific to all employed mobile devices should be developed to ensure compliance. Configuration tests should be developed and executed on all versions of mobile devices under all possible connectivity scenarios to ensure CJIS Security Policy compliance under all expected operating conditions. Since mobile devices can expect to operate in different physical and network environments, testing and validating correct security functions is more critical than on fixed computing platforms. Additionally, security functions that function properly on one version of a mobile operating system on a particular device may not function in the same manner even on the same version on a different device or a different version on the same device.

Media Protection

Some mobile device hardware platforms include the ability to add removable storage in the form of memory cards. This function is primarily related to Android and Windows mobile platforms and is intentionally limited on Apple devices, but may be possible through certain application functions. While the Android platform performs robust cryptographic separation of data stores between applications within the ‘internal’ storage of the device, the Android OS does not provide secure separation of data stores on ‘external’ storage. Some Android hardware devices include additional storage hardwired inside the device that is classified by the operating system as external storage and the normal separation between applications accessing that storage is not applied. Each potential device considered for acquisition must be assessed regarding specific ‘external’ media protection requirements which may actually include built-in media or storage.

Protection of device connected media

As a result of the limited protection and encryption capabilities applied to device removable media and SIM cards for cellular provisioning that include onboard data storage, all externally removable media or memory should be handled consistently with the CJIS Security Policy on media protection.

Encryption for device media

While most mobile operating systems have the capability to encrypt internal storage, it may require specific device settings to be enabled. All mobile device storage should meet the encryption requirements identified for media in the CJIS Security Policy. Specific settings may need to be applied to ensure proper encryption is actually employed. Additionally, the device built-in encryption capability is typically tied to the device PIN or password. Depending on the device PIN or password requirements the integrated encryption may be easily bypassed by password guessing and appropriate consideration should be made to ensure additional encryption protected by advanced authentication methods be applied to all CJI.

Physical Protection

Due to small form factors and the fact that mobile devices are often stored in lower security areas and vehicles, physical protection of the devices must be considered in both policy and training. Physical protections will often be the responsibility of the assigned device user and physical protections typically inherited by individual information systems from a secure facility will not be available to mobile devices which will require compensating controls to achieve compliance.

Device Tracking/Recovery

MDM software as well as some integrated mobile operating system functions may allow tracking of stolen or lost devices via ‘always-on’ cellular data connections and the devices built-in GPS. Device tracking with WiFi only or ‘on-demand’ cellular access may not be reliable. Enabling device tracking capabilities, while not a replacement for secure storage, could be a compensating control used to substantially reduce overall device risk in some scenarios. Device tracking is not currently required in the CJIS Security Policy but should be applied to agency owned devices where possible as a risk mitigation factor. Enabling of device tracking on personally owned devices in a BYOD environment may raise employee privacy concerns and should be considered only for critical systems with the full knowledge of the employee and concurrence of the legal department. This is an enhanced risk that must be accepted for BYOD employments and should be considered

when allowing BYOD employment. Device tracking is available for both limited function mobile operating systems as well as traditional operating systems installed on laptop devices.

Access to device tracking software or applications within the organization should be controlled with limits and formal processes required to initiate a tracking action. It is advisable to include appropriate clauses in user agreements under what conditions and controls the organization applies to device tracking.

Devices utilizing unique device identification/certificates

Devices utilizing unique device identification or have installed certificates may require additional physical protection and/or additional incident handling steps in case of device loss in order to ensure the device unique identifier or certificate is immediately revoked or disabled. Additional physical protection rules or policy would be appropriate for any device which contains access mechanisms tied to the device.

System Integrity (CJIS Policy Section 5.10)

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full feature operating systems. In many cases the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM or EMM application and supporting server infrastructure.

Patching/Updates

MDM software may provide compliance to the Section 5.10.4.1 patch management requirements for particular platforms and software versions. However, devices without ‘always-on’ cellular connections may not be reachable for extended periods of time by the MDM or EMM solution either to report status or initiate patching. Supplementary or manual device accountability methods may need to be implemented to account for devices without persistent connections to ensure their patch and update state is current. Alternatively, some patches or system updates may not be practical over cellular connections and will require connection of devices to a WiFi network. Compliance with CJIS Security Policy requirements through purely technical means may not be practical and considerations should be made for aggressive management of devices through training and mandatory periodic connection of devices to organizationally managed WiFi networks.

TECHNOLOGY NOTE: Apple and Android based devices have different potential issues regarding device operating system updates. Apple maintains support for updating the operating system on Apple hardware for several device generations (typically 3-5 years) and provides a robust mechanism for system updates. However, updates to Android based systems are driven by the individual device manufacturer which may or may not support regular updates to current Android operating system versions. Additionally, different Android device vendors may offer updates/upgrades to the Android operating system on different schedules, which can complicate environments utilizing Android devices from multiple manufacturers.

Malicious code protection/Restriction of installed applications and application permissions

MDM or EMM software will typically allow restrictions on installed applications. One of the few effective attack vectors to compromise mobile operating systems is to manipulate the device user to install a malicious application. Even though the application may be restricted from accessing

other application data, it may have some access to common data stores on the device and access to device functions (e.g. GPS, microphone, and camera) that are undesirable. Unrestricted installation of applications by the device user could pose a significant risk to the device.

Malicious code protection using traditional virus scanning software is technically infeasible on most limited function mobile operating systems that are not rooted or jailbroken. The integrated data and program separations prevent any third party installed program from accessing or 'scanning' within another application data container. Even if feasible, power and storage limitations would be prohibitive in the effect on device battery life and storage capacity on most mobile devices. However, the cryptographic separation between applications and effective application virtualization technologies built into common mobile operating systems partially compensate for the lack of traditional virus scanning technologies. Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a matter analogous to traditional virus scan detection of unauthorized software. This behavior is analogous to the software inventory performed by anti-virus products and can provide a high degree of confidence that only known software or applications are installed on the device. While it is theoretically possible to bypass the application sandboxing and data segregation protections to compromise a mobile device through the web browser, the attack methods required are significantly more advanced than those required for a traditional full featured operating system. Malicious code protections on the device web browser can be enforced through the use of a properly protected web proxy which the device is configured to use as a mandatory device policy. The most common method of malicious code installation is enticing the user to manually install the malicious app which can be mitigated on organizational devices using an MDM or other application installation restrictions which prevent the user from installing unauthorized or unknown applications. Mitigation of this issue within BYOD environments may not be possible and will present a significantly enhanced risk to the device.

TECHNOLOGY NOTE: In the particular area of application installation there is a significant difference between the behavior of Apple iOS and Android platforms. Apple cryptographically restricts the way applications will execute on the device and assigns mandatory application permissions when the application code is signed prior to release on the Apple App Store for distribution. Apps on the Apple platform must conform to Apple's policy on app behavior and cannot exceed their design permissions on access to common device functions once the app has been signed and distributed. However, the Apple method does not typically advertise the precise internal permissions granted to the app to the user prior to installation. At runtime, the app is required to request user permission to access certain device functions, and the user may agree or not agree, which may introduce risk if they are unaware of what they are agreeing to allow. Unsigned or un-trusted apps are cryptographically prevented from executing on non-jailbroken iOS devices. Apple provides a mechanism for organizations to distribute custom apps within an organization with equivalent protections but all receiving devices must have a special certificate installed that will only allow official App Store and the organization custom apps to execute.

Conversely, the Android platform, while also requiring app code signing, allows for self-signed code which can be distributed by means other than an official app store and execute on any Android device. Application permissions are presented to the user once at app installation but ramifications of agreement to certain app permissions may not be obvious to a non-technical user. Permissions in the Android model require user acceptance of all app requested permissions or the app is denied

installation, which can result in unwise user acceptance of excessive permissions in order to gain functionality provided by the app.

On either platform user installation of applications can significantly change the security state of the device. Applications may be able to transmit and receive data or share device common data with other devices over the network or local WiFi or Bluetooth connection. On either platform it is highly desirable to limit allowable applications to a pre-approved pool of apps via MDM or organizational App store structures and device policy. However, the risks associated with uncontrolled app installation is several orders of magnitude greater on Android based devices.

WARNING: Rooted or jailbroken devices are modified in such a manner that the built in protections against malicious code are effectively disabled. A rooted or jailbroken device would require significant and costly compensating controls to achieve compliance.

Firewall/IDS capability

Traditional device or “personal” firewalls as identified in CJIS Security Policy Section 5.10.4.4 may not be practical on limited function mobile device operating systems but significant compensating controls are available. By default, mobile device operating systems have a limited number of system services installed and carefully controlled network access. To a certain extent the mobile operating system performs similar effective functions as a personal firewall would perform on a general purpose operating system. Potential compensating controls for the five (5) personal firewall requirements specified in Section 5.10.4.4 are listed below:

1. Manage Program Access to the Internet: On agency controlled devices with an MDM, limiting the apps installed on the device will effectively perform the same function. Since no software or apps can be installed without MDM approval a robust approval process can effectively ensure internet access is only granted to approved apps. Built-in apps and functions can also be limited on network access by the MDM.
2. Block unsolicited requests to connect to the user device: Default configurations for mobile operating system platforms typically block incoming requests. It is possible to install an app that may ‘listen’ on the network and accept connections, but the same compensating control identified in item 1 will mitigate the likelihood of that occurring.
3. Filter incoming traffic by IP address or protocol: Protocol filtering effectively occurs due to the limited function of the operating sys long as no installed application opens network access ports. The mitigations in 1 effectively compensate for this control as well.
4. Filter incoming traffic by destination ports: Same as 3.
5. Maintain an IP traffic log: This may not be technically feasible on most mobile operating system platforms as maintaining this log would require access to lower level operating system functions that are not accessible unless the device is rooted or jailbroken. However, individual Apps that communicate over the network or accept connections from the network may permit logs of IP traffic associated to that application to be stored.

Spam Protection

Spam guards installed on corporate or organizational email systems may effectively accomplish the spam protection requirements for the CJIS Security Policy on mobile devices if properly configured to block spam before delivery to the device. If no upstream spam guard is installed on the mail server the mobile devices accesses, the device may not have adequate spam protection. Additionally access to internet based email (web mail) would need to be restricted to web mail with appropriate spam and/or antivirus protections to ensure compliance.

Periodic system integrity checks

One method to compensate for the technical infeasibility of traditional anti-virus and malicious code protection is to install an MDM that performs periodic system integrity checks that validate device configuration and status against an approved baseline. Deviations may provide indicators of potential device compromise or mis-configuration.

G.5 Administrator Accounts for Least Privilege and Separation of Duties

Administrator Accounts for Least Privilege and Separation of Duties

PURPOSE:

This appendix is provided to describe industry best security practices for assigning separate administrator accounts to support the concept of Least Privilege.

ATTRIBUTION:

- SANS, "The Critical Security Controls for Effective Cyber Defense", version 5.0
- NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations", Revision 4 dated April 2013
- NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook" dated October 1995
- CNSSI-4009, "National Information Assurance (IA) Glossary", dated April 2010

DEFINITIONS:

Least Privilege – The principle that security architecture be designed to grant individual users and processes only the minimum accesses to system resources and authorizations required to perform their official duties or function.

Separation of Duties – The security principle requiring the division of roles and responsibilities so that a single individual cannot subvert a critical process or function.

SUMMARY:

The implementation of least privilege is accomplished by assigning user or process access to system resources based on operational or business needs. Thus, access is granted to only those resources required to perform assigned duties. For individuals who have multiple roles within the organization requiring varying levels privileges, this assignment of access can be challenging. Often times the agency will assign a single userid to the individual and elevate the privileges for that account based on the different roles. While it may seem logical to allow the user access to all

required resources using a single account, security vulnerabilities can be introduced into the system.

Associated with least privilege is separation of duties. This concept aids in maintaining the integrity of the system by preventing the abuse of elevated privileges for making unauthorized changes to the system. This objective essentially requires different individuals to perform separate functions with relation to (primarily) administrative duties. For instance, those with the ability to create and assign user access to system should not be able to access the audit logs that contain the evidence of the account actions.

USER ACCESS AND ACCOUNT MANAGEMENT:

Several factors influence the manner in which an agency implements and manages user access. Many times, the size of the agency and the technical expertise of the IT staff employed by the agency become primary drivers. Larger agencies with a broad base of technically savvy personnel normally have the ability to dedicate resources specifically to the administration and management of user access. This could translate to the use of multiple accounts for a single user performing duties requiring varying levels of access.

Smaller agencies with few or no technically experienced personnel will often assign single user accounts with the highest level of access required by users. Other smaller agencies may go as far as assigning every user an account with elevated privileges so there are no delays or problems requiring intervention by already overburdened system administrators. It is not uncommon for a smaller agency to outsource system administration duties.

Regardless of the size or resources of an organization, each agency should base the process for assigning access to system resources based on their operational requirements and a thorough risk assessment. To mitigate risk for accessing system resources, industry best security practices prescribe those individuals performing duties requiring elevated privileges be assigned a separate userid to be used in the performance of those duties. This account would be separate from a standard user account.

Why are some agencies unwilling to implement controls for least privilege? One common reason/perception is administrative overhead. There is a time factor for a system administrator to create user accounts and configure those accounts correctly based on the user's role. In larger agencies with many employees, this could add up to a significant impact on the system administrator(s) especially if there is a high level of turnover. Resources in some agencies may allow for a single system administrator dedicated strictly for account management. On the other end of the spectrum, in agencies with fewer employees, the impact may be more burdensome. While there are fewer user accounts to manage, a full-time system administrator for account

management may not be feasible. Those duties then become shared between a few people or added to the duties of a lone person.

Another reason may be the burden on system administrators to remember multiple userids and passwords. This could result in the user using the same password for each account or the user writing down the credentials for ease of remembrance. Additionally, an administrator could get the credentials mixed up between accounts causing an account lockout. This could then require system administrator intervention to reset or unlock the account.

Some agencies may feel that creating additional accounts reduces system resources. Depending on the size of the agency, this could be a concern. In most cases, the number of individuals that would require a secondary account would be minimal. The impact could be limited to a slight increase in disk space usage on the systems accessed by the system administrators with the separate accounts and perhaps the server housing the account information.

THREATS:

A primary goal of attackers is to gain administrative or root privileges on a network or system. Therefore, protection of credentials with that level of access is a key to preventing unauthorized access. Attackers may use many methods in attempts to gain unauthorized, privileged access to computer or network systems. There are two common techniques that take advantage of improperly managed administrative privileges.

Phishing Attacks

In this first method, consider a small organization with limited system administrative resources. Each user is assigned an account with elevated privileges that allows them to perform a myriad of duties including gaining access to critical system security resources. Because this is the only account the user has, normal non-administrative duties are also performed with administrative rights. While checking their email, the user is fooled into reading a message and opening a malicious attachment. Because the user's account has elevated privileges, malware is now installed on the system with elevated privileges. The malware could now allow the attacker to take over the system and install other malicious software such as key loggers, sniffers, or remote control applications. Other key system resources such as firewalls, routers, switches, or intrusion detection systems are now also compromised.

Password Brute Force Guessing / Cracking

The second method may not be as easy as the first and involves the guessing or cracking of passwords on the part of the attacker. Based on human nature, we tend to develop passwords that

are easy to remember and most likely contain some kind of information that is pertinent to us. Some passwords could be easily guessed with a minimal amount of social engineering or fact finding. Consider again an agency that assigns users a single account to perform all duties including those requiring elevated privileges. A user has created a password that, while meeting the requirements of the CJIS Security Policy, is comprised of easily guessed information about the user. An attacker has previously determined the userid and is now able to begin guessing the password. Upon success, the attacker will have unauthorized access to critical system resources.

MITIGATION:

The first step to implementing least privilege is to create separate user accounts for those individuals that require elevated privileges for their duties. These duties could include system or security administration, reviewing audit logs, backup administration, or configuring network devices (e.g. firewalls, routers). The passwords associated with these accounts should have a higher level of complexity than an account without elevated privileges. By disassociating the access levels required for system administration functions from an individual's "everyday use account", should a password be compromised, access would be limited to that of a user with non-elevated privileges.

Second is to implement procedures to ensure accounts with elevated privileges are used only for those duties requiring the higher level of access. This would mean disabling or blocking access to email, web browsers, and other external facing connections. While technical processes are the preferred method of preventing the misuse of accounts with elevated privileges, written policies can be used in situations where technology does not support that type of account management.

Several governance organizations recognize the importance of the security value of Least Privilege. The Payment Card Industry (PCI) includes requirements in their Data Security Standards (DSS). The National Institute of Standards and Technology (NIST) addresses the concept of Least Privilege in its Special Publication (SP) 800-53 rev. 4. While not considered a governance organization, the System Administration, Networking, and Security (SANS) Institute publishes a list of the top 20 security controls which includes "Controlled Use of Administrator Privileges" at number 12. Although the actual security controls or required implementation may slightly differ, the concept is consistent across the groups. The actual controls from NIST and SANS are included here in this appendix.

NIST CONSIDERATIONS FOR LEAST PRIVILEGE:

NIST Special Publication 800-53 rev. 4 includes controls required for all systems under the Federal Information Security Management Act. The publication specifies the guidance for Least Privilege in the control catalog under the Access Control (AC) family and specifically as AC-6. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of

the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-6 is a key control having several enhancements which, when implemented, bolster the overall security of the information system by reducing the risk of compromise through the misuse or misconfiguration of access to system resources.

AC-6 Least Privilege

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

Control Enhancements:

(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

Control Enhancements:

(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions.

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

(3) LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS

The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

(4) LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS

The information system provides separate processing domains to enable finer-grained allocation of user privileges.

Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; (ii) employing hardware and/or software domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32.

(5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].

Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.

(6) LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS

The organization prohibits privileged access to the information system by non-organizational users.

Supplemental Guidance: Related control: IA-8.

(7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES

The organization:

(a) Reviews [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and

(b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.

(8) LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION

The information system prevents [Assignment: organization-defined software] from executing at higher privilege levels than users executing the software.

Supplemental Guidance: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such

applications/programs, those users are indirectly provided with greater privileges than assigned by organizations.

(9) *LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*

The information system audits the execution of privileged functions.

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.

(10) *LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-6 (1) (2) (5) (9) (10)	HIGH AC-6 (1) (2) (3) (5) (9) (10)

**SYSTEM ADMINISTRATION, NETWORKING, AND SECURITY (SANS)
CONSIDERATION FOR LEAST PRIVILEGE:**

There are many negative factors that affect our cyber lives: massive data loss, intellectual property theft, credit card breaches, and identity theft just to name a few. Cyber defense is rapidly evolving to address the plethora of challenges we face. Defenders have access to a wide array of resources to combat those wishing to do harm. Ranging from the collection of vast amounts of intelligence data to security standards to training and certifications, security practitioners are well armed.

But can information overload actually worsen the problem? Organizations must decide, hopefully based on risk analysis, how to wade through all available resources and select those best suited to their own operating environment. The threats continue to evolve, the attackers become smarter, and user access more mobile. The cloud beckons and can provide reduced cost and infrastructure at a price of less control and accountability for vital information.

The SANS Institute publishes the “20 Critical Security Controls for Effective Cyber Defense”. This list of controls is the combined result of work by an international community to create, adopt, and support the controls. The components of the community provide insight, tools, information, and solutions into threats and adversaries. This list includes the control titled “Controlled Use of Administrative Privileges”. SANS describes this control as: *The process and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

Critical Security Control (CSC) 12: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

ID #	Description	Category
CSC 12--1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	<i>Quick win (One of the “First Five”)</i>
CSC 12--2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive	<i>Quick win</i>
CSC 12--3	Configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, and with no dictionary words present in the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length.	<i>Quick win</i>

CSC 12---4	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration---level accounts.	<i>Quick win</i>
CSC 12---5	Ensure that all service accounts have long and difficult--- to--- guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords.	<i>Quick win</i>
CSC 12---6	Passwords should be hashed or encrypted in storage. Passwords that are hashed should be salted and follow guidance provided in NIST SP 800---132 or similar guidance. Files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super---user privileges.	<i>Quick win</i>
CSC 12---7	Utilize access control lists to ensure that administrative accounts are used only for system administration activities, and not for reading e---mail, composing documents, or surfing the Internet. Web browsers and e---mail clients especially must be configured to never run as administrator.	<i>Quick win</i>
CSC 12---8	Through policy and user awareness, require that administrators establish unique, different passwords for their administrative and non---administrative accounts. Each person requiring administrative access should be given his/her own separate account. Users should only use the Windows “administrator” or UNIX “root” accounts in emergency situations. Domain administration accounts should be used when required for system administration instead of local administrative accounts.	<i>Quick win</i>
CSC 12---9	Configure operating systems so that passwords cannot be re--- used within a timeframe of six months.	<i>Quick win</i>
CSC 12---10	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators’ group, or when a new local administrator account is added on a system.	<i>Visibility/ Attribution</i>
CSC 12---11	Configure systems to issue a log entry and alert when unsuccessful login to an administrative account is attempted.	<i>Visibility/ Attribution</i>

CSC 12---12	Use multifactor authentication for all administrative access, including domain administrative access. Multi--- factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.	<i>Configuration/ Hygiene</i>
CSC 12---13 (NEW)	When using certificates to enable multi---factor certificate---based authentication, ensure that the private keys are protected using strong passwords or are stored in trusted, secure hardware tokens.	<i>Configuration/ Hygiene</i>
CSC 12---14	Block access to a machine (either remotely or locally) for administrator---level accounts. Instead, administrators should be required to access a system using a fully logged and non---administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems. Users would use their own administrative accounts and enter a password each time that is different than their user account.	<i>Configuration/ Hygiene</i>

Quick win: Implementation provides significant risk reduction without major financial, procedural, architectural, or technical changes to an environment, or that provide substantial and immediate risk reduction against very common attacks that most security-aware organizations prioritize these key controls.

Visibility / attribution: Measures to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

Configuration / hygiene: reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.

SEPARATION OF DUTIES:

Separation of duties is another security control related to least privilege. Many of the same challenges faced by least privilege apply to this concept as well. Agency size and resources play a major in the implementation of separation of duties. As the name implies, some key functions should be separated between different individuals. The goal of this concept is to provide protection

against a single individual's ability to circumvent system security controls to gain unauthorized access or perform unauthorized actions without colluding with other individuals.

Simply put separation of duties entails distributing certain critical mission oriented functions or system administrative support functions amongst different individuals or roles. It also includes delineating information system support duties such as auditing, configuration control, or network security between different individuals.

As with least privilege, an agency's ability to implement separation of duties is typically based on financial and personnel resources. While a very large agency may have ready availability to those resources to ensure critical functions are spread across multiple individuals, a small agency probably does not have that luxury.

THREATS:

What effect can an individual with carte blanc access to all critical functions of a system have? Consider a single individual with the ability to install nefarious applications on a system (e.g. a keylogger). If this same individual also has the ability to edit any audit logs that would have recorded the actions of installing the software, those entries could be deleted and any evidence of the installation eliminated.

Perhaps a disgruntled system administrator wants to open a port on a firewall to allow a remote backdoor connection into the information system in order to siphon off criminal justice information. Because the perpetrator has access to the firewall and all logs, the port can be opened and the logs tampered with to eliminate records of the action.

As mentioned previously, the two concepts of least privilege and separation of duties are related. Additional threats are presented when a system administrator using a single account with unlimited elevated privileges across the information system uses that account to check email. In a successful phishing attack that compromises this account, the attacker now has unrestricted unauthorized access to all system resources and the ability to hide their tracks.

MITIGATION:

The primary method to avoid these situations is to configure system privileges and duties such that a single person is unable to effect questionable change to the system and then are able to erase any evidence of the change.

Technical configurations are most secure and sound enforceable policies compliment the technical solutions. When an information system does not support separating duties, strong policies help mitigate risk.

NIST CONSIDERATIONS FOR SEPARATION OF DUTIES:

NIST Special Publication 800-53 specifies the guidance for separation of duties in the control catalog under the Access Control (AC) family and specifically as AC-5. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-5 is a relatively small control with no enhancements but it is significant in protecting the integrity of an information system.

AC-5 Separation of Duties

Control: The organization:

- a. Separates [*Assignment: organization-defined duties of individuals*];
- b. Documents separation of duties of individuals; and
- c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-5	HIGH AC-5

G.6 Encryption

Encryption

Purpose:

This paper was created to provide assistance and guidance on encryption types, methods, and to provide general best practices in the implementation of encryption.

Attribution:

- FIPS 140 – 2, Security Requirements for Cryptographic Modules (May 2001)
- FIPS 197, Advanced Encryption Standard (Nov 2001)
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
- CNSSP-15, National Information Assurance Policy on the Use of Public Standards for Secure Sharing of Information among Security Systems
- CJIS Security Policy

Definitions and Terms:

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Decryption – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Asymmetric Encryption – A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Symmetric Encryption – A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

Hybrid encryption – A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Authorized User/Personnel - An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Summary:

CJIS Security Policy encryption requirements are intended to provide protection of the sensitive data that is criminal justice information (CJI). The primary goal of encrypting CJI is to prevent unauthorized access to this sensitive data. Encryption is a great tool that can be applied to accomplish this protection and ensure compliance with the vast majority of the CJI requirements. CJIS Security Policy Section 5.10.1.2 details when encryption is required and provides information on the exceptions to the encryption requirement.

Achieving CJIS Security Policy Compliance:

To determine when encryption is required one must first read and understand CJIS Security Policy Section 5.9.1 Physically Secure Location. The reason for this is simple: encryption is not required while within a physically secure location. Conversely, whenever CJI is transmitted or stored (at rest) outside the boundaries of a physically secure location encryption may be required. The exact standards to which the data would be required to meet are detailed along with any exceptions in CJIS Security Policy Section 5.10.1.2.

Additionally, both security awareness training and personnel security requirements can be affected by whether or not CJI is encrypted. Requirements surrounding these Policy areas is determined by answering the following question: Who has unescorted access to unencrypted CJI?

Unless personnel is escorted, security awareness training is required as correlated with the access level needed by personnel as identified in CJIS Security Policy Section 5.2. Similarly, fingerprint-based background checks as detailed in CJIS Security Policy Section 5.12 may be required on individuals to permit unescorted access to CJI.

The intent of all these requirements is to limit access to CJI to only authorized personnel. CJIS Security Policy Appendix A: Terms and Definitions defines authorized user/personnel as an individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

What is Encryption?

Encryption is the process of encoding messages or information in such a manner that only people with the knowledge or means to decrypt the message can do so. But how does this work?

In an encryption process, legible data, referred to as plaintext, is encrypted by applying a cipher (otherwise known as an encryption algorithm or crypto key) to the data. The data then becomes encrypted and is now referred to as ciphertext. The ciphertext is essentially unreadable until decrypted. The decryption process requires the process of applying the same algorithm (crypto key) to encrypt the data in an inverse manner to convert the data back into plaintext.

Encryption is important because it allows you to securely protect data that you don't want anyone else to have access to. Encryption has been used throughout history to send “secrets” securely by some form of obfuscation to a recipient. Businesses and enterprises use encryption to protect corporate secrets and sensitive employee data, such as payroll information and personally identifiable information (PII). Governments secure classified information with encryption. Additionally, individuals may use encryption to protect personal information, such as credit card data, banking information, and passwords to guard against things like identity theft.

It should be known that encryption may not always prevent the interception of data. If the stolen data is encrypted, though, it would be extremely difficult for any of the data to be decrypted without having the decryption key. While it may be possible to decrypt the message without possessing the key, it does require large computational resources, great skill, and lots of time to accomplish such a task. Exercising encryption along with key management policies is one of the best security practices that can be put into place with regard to sensitive data security and protection.

Types of Encryption:

Symmetric Encryption

Symmetric encryption is also commonly known as secret key encryption. Symmetric encryption is a form of cryptography utilizing a singular encryption key to guise an electronic message. Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message. Symmetric encryption is a two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key.

Symmetric encryption is most often used for data protection whether at rest or in transit, especially in bulk, due to the ease and speed with which the encryption can be implemented. The most common examples of symmetric algorithms are: AES and Triple-DES (3DES or TDEA).

How it works:

To encrypt and send a message to Jane, John does the following:

1. Generates a new symmetric key
2. Encrypts the message using this new symmetric key
3. Sends the message to Jane
4. Sends the encrypted symmetric key to Jane - out of band

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Receives the symmetric key
3. Uses the symmetric key to decrypt the message

Asymmetric Encryption

Asymmetric encryption is also commonly known as public-key encryption. Asymmetric cryptography is cryptography in which a pair of keys, a public key and a private key, are used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

Creating Key Pairs:

Asymmetric encryption requires the use of algorithms of great computational complexity to create the key pairs. This is accomplished by using a large, random number that an algorithm is applied to which generates a pair of keys for use as asymmetric key algorithms (as shown in Figure 1 below).

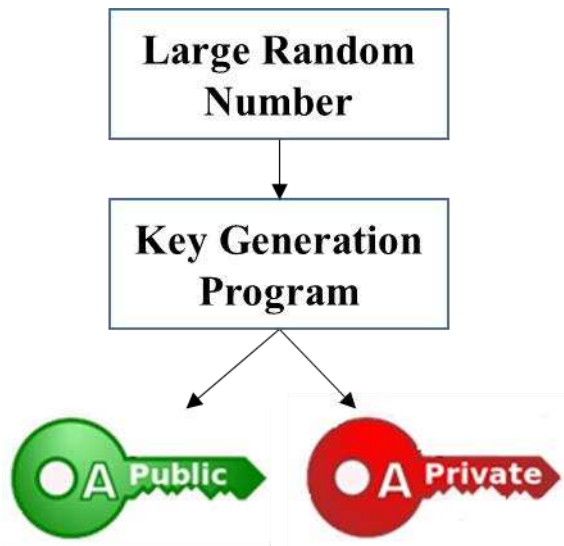


Figure 1 – Asymmetric key pair generation

Asymmetric encryption is most often used to encrypt a single message before transmission. The most common examples of asymmetric algorithms are: RSA and DSA.

How it works:

To encrypt and send a message to Jane, John does the following:

1. Obtains Jane's public key
2. Encrypts the message using Jane's public key
3. Sends the message to Jane

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Uses her private key to decrypt the message

Advantages of Using Symmetric Encryption for Data Protection

Asymmetric encryption requires the use of algorithms with great computational complexity to create the key pairs, and therefore is not practical for large amounts of data. It is typically used for only for short messages. Also, asymmetric encryption must use a comparatively stronger key than symmetric key encryption to achieve the same level of protection as one key (public) will be published in the public directory for all to see.

Symmetric encryption is based on large, but simple algorithms which require less computation. Therefore, is much faster to create and use keys. This allows the same key to be used to encrypt and decrypt the message. So, data can be encrypted in real time. The (shared) key is sent to the recipient out of band so that it can be used to decrypt the data.

For the reasons stated above, symmetric key encryption is the preferred choice by both industry and government alike to encrypt large amounts of data (bulk encryption) simply due to the ease and real time encryption capabilities as detailed above. Additionally, a new key can be generated for every session, message transaction, etc., as desired. This means a sender won't have to use one key (public) to encrypt a message and have the recipient use another key (private) to decrypt the message.

Hybrid Encryption

Hybrid encryption solution exist where both asymmetric encryption and symmetric encryption keys are used to create what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Hybrid solutions are most often used by Internet browsers to protect data in transit. The most common examples of hybrid encryption are: TLS/SSL, PGP, IPSEC, and S/MIME.

How it works:

To encrypt a message to Jane in a hybrid cryptosystem, John does the following:

1. Obtains Jane's public key
2. Generates a new symmetric key
3. Encrypts the message using this new symmetric key
4. Encrypts the symmetric key using Jane's public key
5. Sends the message to Jane

To decrypt this hybrid cipher text, Jane does the following:

1. Receives the encrypted message
2. Receives the encrypted symmetric key
3. Uses her private key to decrypt the symmetric key
4. Uses the symmetric key to decrypt the message

Explaining Cipher Suites:

A cipher suite is a set of cryptographic algorithms used for the following:

- Protect information required to create shared keys (key exchange)
- Encrypt messages exchanged between clients and servers (bulk encryption)
- Generate message hashes and signatures to ensure the integrity of a message (message authentication)

Examples of Transport Layer Security (TLS) 1.2 Cipher Suites:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

A cipher suite specifies one algorithm for each of the above tasks. For example, the TLS_RSA_WITH_AES_128_SHA256 cipher suite is used for TLS. The suite uses the RSA asymmetric algorithm for key exchange, AES with a 128-bit key for bulk data encryption, and SHA256 for message authentication.

Symmetric and Asymmetric Key Strength Comparison:

<u>Symmetric</u>		<u>Asymmetric</u>		
<u>Bits of security</u>	<u>Symmetric key algorithms</u>	<u>Finite-Field Cryptography (FFC)</u> <u>(e.g., DSA, D-H)</u> <u>Bits of security</u>	<u>Integer-Factorization Cryptography (IFC)</u> <u>(e.g., RSA)</u> <u>Bits of security</u>	<u>Elliptic-Curve Cryptography (ECC)</u> <u>(e.g., ECDSA)</u> <u>Bits of security</u>
<u>80</u>	<u>2TDEA18</u>	<u>Public key = 1024</u> <u>Private key = 160</u>	<u>Key size = 1024</u>	<u>Key size = 160-223</u>
<u>112</u>	<u>3TDEA</u>	<u>Public key = 2048</u> <u>Private key = 224</u>	<u>Key size = 2048</u>	<u>Key size = 224-255</u>
<u>128</u>	<u>AES-128</u>	<u>Public Key = 3072</u> <u>Private key = 256</u>	<u>Key size = 3072</u>	<u>Key size = 256-383</u>
<u>192</u>	<u>AES-192</u>	<u>Public key = 7680</u> <u>Private key = 384</u>	<u>Key size = 7680</u>	<u>Key size = 384-511</u>
<u>256</u>	<u>AES-256</u>	<u>Public key = 15360</u> <u>Private key = 512</u>	<u>Key size = 15360</u>	<u>Key size = 512+</u>

Figure 2 - Symmetric and asymmetric key strength comparison

As you can see in the chart provided above, the equivalent key strengths between symmetric and asymmetric key strengths do not necessarily correlate. There is a reason for this. As stated previously, asymmetric algorithms must use a comparatively stronger key than symmetric key encryption to achieve the same strength. The simplest explanation for this is because one of the keys is published to the public directory and can constantly be attacked by anyone with access to the directory. Therefore, the public key must be made of such strength that it can resist getting compromised while made public.

Federal Information Processing Standard (FIPS) 140-2 Explained

Origin of FIPS 140-2

On July 17, 1995, the National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) to validate cryptographic modules to Federal Information Processing Standards (FIPS) Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC). FIPS 140-2, Security Requirements for Cryptographic Modules, was released on May 25, 2001 to supersede the original FIPS 140-1. Modules validated as conforming to FIPS 140-1 and FIPS 140-2 are accepted by the Federal Agencies of both countries for the protection of sensitive information.

What is FIPS 140-2?

Federal Information Processing Standard (FIPS) is a standard developed and recommended (often mandated) for use in federal-government-operated IT systems by the following two government bodies:

- The National Institute of Standards and Technology (NIST) in the United States
- The Communications Security Establishment (CSE) in Canada

FIPS 140-2 specifies the security requirements a cryptographic module must meet when utilized within a security system protecting sensitive information within information systems (computer and telecommunication systems). FIPS 140-2 specifies which encryption algorithms can be used and how encryption keys are to be generated and managed.

How does a product get certified?

Vendors of cryptographic modules can have their products tested by independent, accredited Cryptographic and Security Testing (CST) laboratories. The CST laboratories use the Derived Test

Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules against the applicable standards in a variety of implementations. The result of these tests are reported to NIST's Computer Security Division (CSD) and CSEC who jointly serve as the Validation Authorities for the program. These results are then reviewed and certificates would be issued if the results are determined to be acceptable.

What is the difference between being FIPS 140-2 compliant and being FIPS 140-2 certified?

It is common theme to discover a product is “FIPS compliant.” What does this mean, though? The difference between compliance and certification is not subtle. Certification requires a vast testing, verification, and validation process be performed by a CST laboratory as described in the previous section. Compliance is merely a claim stating the implementation of an encryption solution is done in accordance with the security policy related to the FIPS certification. Any claim of compliance would need to be validated and the corresponding certificate number would have to be known.

NIST has addressed related claims as shown below in their Frequently Asked Questions for the Cryptographic Module Validation Program:

A vendor makes the following claims of conformance to FIPS 140-2. Are they acceptable?

- The module has been designed for compliance to FIPS 140-2. <NO>
- Module has been pre-validated and is on the CMVP pre-validation list. <NO>
- The module will be submitted for testing. <NO>
- The module has been independently reviewed and tested to comply with FIPS 140-2. <NO>
- The module meets all the requirements of FIPS 140-2. <NO>
- The module implements FIPS Approved algorithms; including having algorithm certificates. <NO>
- The module follows the guidelines detailed in FIPS 140-2. <NO>
- The module has been validated and has received Certificate #XXXX. <YES>

A cryptographic module does not meet the requirements or conform to the FIPS 140-2 standard unless a reference can be made to the validation certificate number. The module used must also be the same version/part number as annotated on the validation certificate. Any other claims are not relevant.

To read more FAQs from NIST on FIPS certification, use the following NIST website link:
<http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPFAQ.pdf>

Where can I learn more about FIPS 140-2?

For more information about the FIPS 140-2 standard, go to the following NIST website:
<http://csrc.nist.gov/cryptval/140-2.htm>

General Recommendations:

Encryption key management control is of paramount importance! Agencies should develop policies and procedures define and monitor the administrative tasks involved with protection, storage, organization, access controls and the lifecycle management of encryption keys. After all, encryption keys should not be accessible by just anyone. An encryption key management control process should ensure only authorized users have access to encryption keys. Key management is a best security practice and helps to ensure the confidentiality and integrity of CJI data and enforces key access control.

The CJIS Security Policy is a “living” document under constant review and receiving regular updates through the Advisory Policy Board (APB) process. Agencies need to always keep up to date on the latest requirements. These requirements can be found in CJIS Security Policy Section 5.10.1.2. Please contact the CJIS ISO Program anytime to address any questions or concerns about CJIS Security Policy requirements, the current APB status of CJIS Security Policy requirements, or if seeking general information or guidance.

G.7 Incident Response

Incident Response

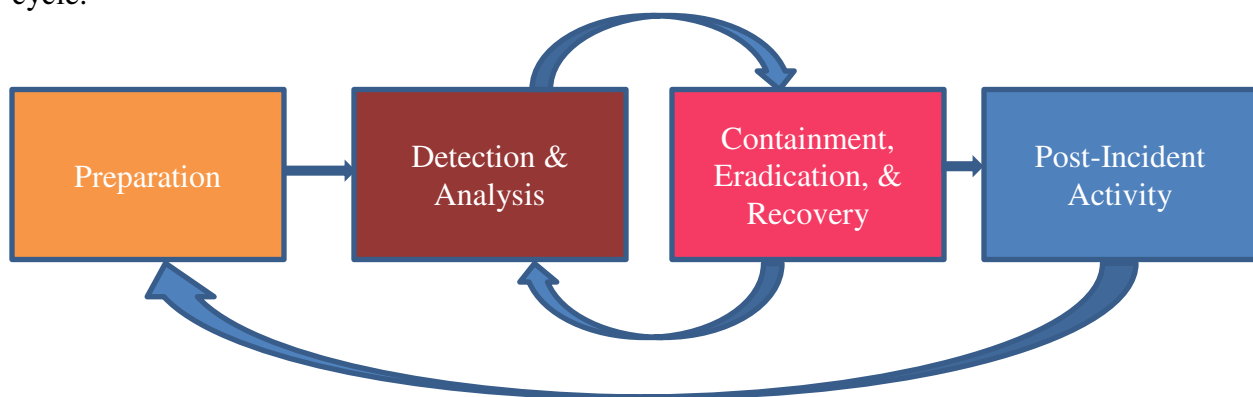
Introduction

Information technology (IT) security incident response is an important and critical component of information technology programs. Performing incident response effectively can be a complex undertaking – for that reason, establishing a successful incident response capability requires planning and resources. Everyone in an organization must be aware of IT security risks, threats, and actions to take in situations where an actual IT security incident has occurred. Even the best-secured and controlled environments can experience these security risks, threats, events, and incidents. This document provides guidelines for appropriate response to IT security incidents, and are independent of specific hardware platforms, operating systems, protocols, or applications.

The following example incidents are used to highlight appropriate actions during each phase:

- Malicious code execution
- Ransomware execution
- Denial of service attack
- Social Engineering
- Phishing

NIST Special Publication 800-61 rev. 2 outlines the “Incident Response Life Cycle” as a collection of phases – distinct sets of activities that will assist in the handling of a computer security incident, from start to finish. The following diagram explains the process flow of the incident response life cycle:



Preparation

The initial phase of the incident response life cycle, “Preparation”, involves establishing and training an incident response team, and acquiring the necessary tools and resources. A computer security incident may not have happened at this phase, but it is important to utilize all available knowledge and security measures to obtain the best posture for responding to potential future incidents. One of the most important preparation steps involves the collection, storage, and accessibility of event data and telemetry from hardware and software resources such as firewall logs, application logs, operating system logs, and other valuable sources of situational data, as well as the output of products that perform analysis on such data. Preventive measures to mitigate or eliminate future incidents are deployed during this phase, using industry best practices, data obtained from research and intelligence sources, and lessons learned from past incidents.

It is also imperative to prepare a list of contact information or notification methodologies to employ when an incident occurs, as well as notification and communication strategies within the team, with stakeholders, and with upper management and potentially other criminal justice and non-criminal justice agencies. This will help ensure that when incidents arise, the proper personnel and organizations are notified and kept informed of the circumstances regarding the incident.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Preparation phase can be given:

Malicious code execution

Preparation for incidents involving malicious code execution should initially involve user awareness of sources of malicious code. There are many potential sources of malicious code, such as web pages, emails, and removable media. The utilization and deployment of effective antivirus software, integrity-monitoring software, and intrusion detection and prevention software are effective measures to take to prepare for incidents involving malicious code execution.

Ransomware execution

Preparation phase activities for incidents involving ransomware execution are much the same as activities for malicious code execution, as ransomware is a specialized form of malware that encrypts potentially important or critical files, with the intention of coercing a victim to pay for a decryption key. Implementing a robust offline backup solution for these types of files is an important preparative action to take regarding the execution of ransomware. This will ensure that when ransomware attacks do happen, the mission impact is as minimal as possible and very little or no data is lost.

Denial of service attack

Denial of service attacks are given attention in the preparation phase. Defensive responses to denial of service attacks typically involve the use of a combination of attack detection and traffic classification and response tools, aiming to block traffic identified as abusive denial of service activity. Deploying solutions such as IDS/IPS devices and software, network hardware with rate-limiting capabilities (routers, switches, and firewalls), and upstream filtering devices at the system perimeter can mitigate for denial of service attacks.

Social Engineering

Preparation for social engineering attacks starts with user awareness training. Understanding and identifying attempts to obtain information in an unauthorized manner is crucial to thwarting these types of scenarios. Social engineering is the art of manipulating people to obtain information they may not be authorized to handle. Training and routinely testing users on potential social engineering scenarios and tactics, and providing training regarding appropriate responses to requests involving personal or otherwise sensitive information (for example, passwords or criminal justice information), is an effective way to ensure social engineering attacks never traverse past the preparation phase of the incident response life cycle.

Phishing

Like social engineering, preparation for phishing attacks is imperative. Phishing is a social engineering technique attackers employ to deceive users, in a fraudulent attempt to obtain sensitive information, or to gain unauthorized access to systems. Phishing is extremely widespread, and attackers disguising fraudulent scenarios in electronic communication such as email and instant messages are the most common. User awareness of these types of tactics is paramount to prepare for phishing attacks and schemes.

Detection and Analysis

The detection and analysis phase begins when a security incident has occurred. To understand when this phase begins, there must be a capability for an intelligent determination of circumstances constituting a security incident. Specialized knowledge and highly trained personnel are necessary for this step to be effective. Many organizations employ teams of personnel who are specifically trained to handle the intricacies of the incident response life cycle. The determination of a security incident can arise from one or several circumstances simultaneously – for example:

- Trained personnel manually reviewing collected event data for evidence of compromise
- Software applications analyzing events, trends, and patterns of behavior
- The observation of suspicious or anomalous activity on a computer system

The goals of this phase are:

- To detect whether a security incident occurred
- To determine the vector (i.e., method) of attack
- To determine the impact of the incident to the mission, systems, and personnel involved in the incident
- To obtain or create intelligence products regarding attack vectors and methodologies, especially when dealing with malicious code

Prioritization of incidents is also an important decision point in the incident response life cycle, as the circumstances regarding an incident can bring the situation to a critical level. There are three major impacts to consider when addressing priority of incidents:

- **Functional Impact:** the impact to business functionality
- **Information Impact:** the impact to confidentiality, integrity, and/or availability of criminal justice information
- **Recoverability:** the amount of time and resources that must be spent on recovering from an incident

Documentation regarding an incident should be thorough and applicable to the incident. This can be crucial in incidents that may lead to legal prosecution, as well as being invaluable to efficiently document, track, handle, manage, and resolve one or more incidents at the same time.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Detection and Analysis phase are given:

Malicious code execution

Detection of malicious code execution is often a primary job of host-based antivirus software. Having a capable and up-to-date antivirus solution installed on a system can detect known malicious code, as well as detect potentially malicious behaviors. The delivery of malicious code to a system can be detected by network traffic analysis and protection tools and hardware. Additionally, some malicious code may produce network traffic that is indicative of successful execution, exploitation, and/or compromise of a system. Solutions such as intrusion detection/prevention systems, Security Information and Event Management (SIEM) tools, and file integrity monitoring software can provide the necessary level of fidelity to make a determination of malicious code execution.

Knowing if or when a system is infected is not always immediately evident. Security controls may have been bypassed or even disabled by the malicious code. However, systems infected by malicious code or software (i.e. malware) can exhibit several indicators. These indicators include, but are not limited to:

Unexpected pop-up windows

- Slow start up and/or slow performance
- Suspicious hard drive activity including an unexpected lack of storage space
- Missing files
- Crashes and/or error messages
- Unexplained network activity
- Hijacked email

Analysis of malicious code can be performed in several ways. Static analysis of malicious code can be performed to determine the capabilities of the malicious code and generate actionable intelligence. Dynamic analysis of malicious code can be used to observe how the malicious code interacts with the system and what actions it performs and can often more rapidly determine the capabilities of malicious code. Both static and dynamic analysis can be performed manually, as well as in an automated fashion. Trained specialized personnel are crucial to the analysis of malicious code.

Ransomware execution

The detection of ransomware is identical to the detection of malicious code. Ransomware is specialized malicious code that encrypts potentially valuable files, generally with the intent to coerce a victim to pay a ransom for the possibility of the decryption of those files. Host-based antivirus solutions can also detect these threats, and network traffic analysis and protection tools and hardware can be used to prevent the successful execution of ransomware. SIEM tools and file integrity monitoring software can also detect the execution of ransomware.

Analysis of ransomware is identical to the analysis of malicious code, and the same intelligence can be determined in the same fashion as with the analysis of malicious code. The most obvious sign that ransomware has affected a system is the existence of encrypted files, the disappearance of certain types of files, and/or the presence of “ransom notes” on the system, which contain instructions for payment to obtain a decryption key, which may or may not be legitimate.

Denial of service attack

Denial of service (DoS) attacks are often detected at the perimeter of an organization but can also be detected within the organization as well. Often, from a user’s perspective, the signs of a DoS attack appear to be network performance or administrative maintenance related issues such as slow or broken network connections or down websites. Additionally, an administrator may notice ping time outs, event logs overflowing or alerts from network monitoring systems as issues that may identify a DoS attack. Intrusion detection and prevention software and platforms can detect denial of service attacks, as well as some network monitoring hardware and appliances, such as web application filters, routers,

firewalls, and switches. Devices targeted by denial of service attacks can also detect the attacks in some instances, if they have the capabilities to determine explicit attack activity versus normal network traffic.

Analysis of denial of service attacks include the determination of the source traffic, the protocols used to generate the traffic, the service(s) targeted by the attack, and the potential impacts of the attack. Network monitoring devices can often provide these types of data, with the exception of potential impacts of denial of service attacks on systems.

Social Engineering

Detection of social engineering attacks is primarily based on the situational awareness of the individual targeted by social engineering. Given that social engineering is a broad topic that can involve the manipulation and exploitation of people in control of an information system, user awareness of social engineering attempts is crucial. If the target has security awareness training in detecting attempts to gain information or access in an unapproved manner, social engineering is easier to detect.

Analysis of social engineering attacks will generally rely on the recollection abilities of or documentation taken by the targets of the attack. Social engineering may not occur on an information system and may be completely carried out in-person. If the target can recollect or produce documentation regarding the social engineering attempt, the motivation and desired access can potentially be determined. For successful social engineering attempts, recollection and documentation of the attempt is crucial to determining the level of unauthorized access that was obtained.

Phishing

Detection of phishing attacks generally will first occur at an organization's email point of presence. Some organizations still run their own email servers, and many have migrated to cloud solutions. Having an on-premise email server or server farm or cluster will require additional functionality to detect phishing attempts. For example, the header content of the email will need to be read, as well as the content inside the body of the email, to check for potentially malicious content and potentially falsified data that may indicate a phishing email. Many cloud email providers have built this capability into their email solutions, but it is still possible for users to receive phishing emails, as attacker tactics and capabilities evolve daily. The most effective detection of phishing comes from heightened situational awareness of potential attacks. Validating the source of the email can uncover potential phishing attempts.

Analysis of phishing attacks involves examination of email headers, as well as contents of the body of the email. The body of the email may contain malicious content, attachments, or links to suspicious or malicious content. Manual or automated analysis activities can be

performed on the email content. Analysis of these elements should be performed by trained specialized personnel to generate intelligence and aid with the determination of indicators of compromise.

Containment, Eradication, and Recovery

Containment activities for computer security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident. Often, this requires intelligence gathered by the detection and analysis phases of the incident – for example, identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels can be invaluable to the implementation of containment activities. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of the strategy is delayed.

Eradication efforts for a computer security incident involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

Recovery efforts for incidents involve restoration of affected systems to normal operation. This may include actions like restoring systems from backups, rebuilding systems from an agency-approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security.

Compromised hosts are often attacked during these phases, as attackers try to regain their foothold on compromised systems or systems on the same network or others in the logical vicinity.

Malicious code execution

Containment activities for malicious code execution involve the logical or physical isolation of the host from the attacker's control and from any mission services or systems that would be impacted by the compromised host. This may include putting the host in a restricted VLAN, using firewalls to block traffic, disconnecting it from the network completely, shutting it down, or disabling functionality. Exercise caution as malicious code may have capabilities to take further actions on a host in case communications with a command and control server are severed. It is important to understand the capabilities of the malicious code before taking containment actions.

Eradication activities include the removal of malicious code from the system. This may be as simple as removing files, configuration rules, accounts, and other persistent items that the malicious code utilizes to function and maintain a presence on the system. This phase

also involves the discovery and removal of indicators of compromise on other systems, if applicable. It is imperative to remediate vulnerabilities that may have been exploited during eradication as well.

Recovery from malicious code execution generally is similar across many environments. Rebuilding the system from a clean baseline or restoring files from backup are typical activities that help restore the functionality of the system to continue the mission. Changing system passwords, installing patches, implementing tighter network access control, and ensuring appropriate levels of logging fidelity of the information system are integral parts of the recovery process.

Ransomware execution

Containment for ransomware execution should be as swift and immediate as possible, as ransomware can execute and spread to accessible media at a rapid pace. Considering files are being encrypted or have already been encrypted, immediate action should be taken to logically or physically isolate the system by disconnecting network connectivity. It is up to the system owner whether to take the risk in powering off the system, as valuable forensic artifacts may be destroyed in the process, but it will halt the execution of the ransomware and protect potentially valuable files. Please note that containment of active ransomware execution is one of the only circumstances where measures such as immediate shutdown are recommended.

Eradication of ransomware does not need to occur in most circumstances, as the entire goal of ransomware is to encrypt files and leave “recovery” instructions to extort victims. The vast majority of ransomware will delete itself once encryption of files is complete, but it is possible that some ransomware is persistent and can remain on the system. If this is the case, analysis should be performed on the ransomware to determine its capabilities, and eradication activities will proceed in an identical fashion to malicious code execution eradication activities.

Recovery from ransomware execution involves restoring encrypted files from backup and may involve the rebuilding of an entire system depending on the extent of the encryption from the ransomware. If a robust offline backup solution for hosts is not present or not utilized on a regular basis, the loss of potentially valuable data may be incredibly costly in several areas to repair, to include man-hours, revenue, and business products, data, and intelligence.

Denial of service attack

Containment of denial of service attacks involve the modification of access control where the attack is occurring. For example, if a web or application server is experiencing a denial of service attack, the system itself, as well as network monitoring devices, should be

examined to determine the source of the attack traffic. Once the source of the traffic is identified, modifications to access controls or rate-limiting features such as firewall access controls lists (ACLs) and web application filters can be employed to block the traffic. Care must be taken to determine if the observed traffic is actually intentional malicious denial of service traffic, versus heavy legitimate network traffic. Implementing access control mechanisms or rate-limiting features may negatively affect the mission of the system. It is also important to note that manual containment in this fashion may not be entirely effective, as attackers can circumvent the ACL by changing the attacking IP address, protocol, or other attribute of the connection.

Eradication is not necessarily applicable in denial of service scenarios, unless a vulnerability or misconfiguration is being exploited to cause the denial of service condition. If this is the case, take steps to remediate the vulnerability or misconfiguration.

Recovery actions depend on the available resources of the information system. For example, on-premise load balancers can be used to distribute the traffic, whether legitimate or malicious, to other less-burdened systems. Many cloud providers and content delivery networks also have denial of service mitigation capabilities. It may also be prudent to increase the resources (memory, processing capacity) of internet-facing systems so that they can handle larger amounts of traffic simultaneously.

Social Engineering

Containment regarding social engineering attacks is dependent upon the information or access that was provided to the attacker. For example, if an attacker gained access to an account on a system following a social engineering attempt, the account should be administratively disabled and all sources of event data regarding that account should be immediately collected. If sensitive data was divulged to the attacker, the impact of the exposure of that data should be examined and mitigating activity should be initiated to determine or reduce the damage of the spread of the information.

Eradication regarding social engineering attacks also depends on the information or access provided to the attacker. Removing or limiting the provided access is a pertinent eradication action. If the information provided is a credential to a system, disable and remove the credential from the system. Eradication may also involve the physical detainment or removal of personnel from a site.

Recovery actions for social engineering attacks are dependent on the information or access provided to the attacker. Additionally, security awareness training is an appropriate recovery action to ensure staff understands the threats of social engineering.

Phishing

Containment of phishing activity is tied very closely to the identification and analysis of the phishing activity. Understanding the tactics of the phishing attacker is paramount to deploying containment activities. Activities include, but are not limited to, administratively blocking sender email addresses and IPs, blocking potential malicious content in email via a web proxy, communicating with potential recipients, and implementation of email content or hyperlink blacklisting if possible. Phishing attacks can also include attempts to have users execute malicious code on systems, where containment activities regarding malicious code will be applicable.

Eradication of phishing attacks include the administrative removal of the emails from email systems, as well as eradication actions for malicious code if applicable.

Recovery from phishing attacks can include:

- Implementation and enforcement of the Domain Keys Identified Mail (DKIM) email authentication method, which can mitigate the possibility that attackers can send spoofed email
- Implementation and enforcement of Sender Policy Framework (SPF) to control and stop sender forgeries
- Implementation and enforcement of Domain-based Message Authentication, Reporting, and Conformance (DMARC), which enables message senders to indicate that their messages are protected with SPF and/or DKIM

Additionally, if malicious code is present in the phishing attack, recovery actions regarding malicious code may be applicable.

Post-Incident Activity

Post-incident activities occur after the detection, analysis, containment, eradication, and recovery from a computer security incident. Arguably one of the most important phases of incident response, post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Some of the important items to consider:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?

- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar actions in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Smaller incidents, and those that are similar to others that have been well documented, do not necessarily need much focus in this phase of incident response. Larger and less-understood security incidents should be the focus of a comprehensive post-mortem evaluation that outlines many of the items listed above and should include personnel that can have a direct impact on or are directly affected or responsible for the involved systems.

Post-incident activities such as these also help to serve as training opportunities for all parties involved in the incident, from victims, to system administration personnel, to incident responders.

Malicious code execution

Post-incident activities for malicious code execution generally will follow similar patterns. A timeline of activity should have been prepared using digital forensic data collected during the detection and analysis phases of the incident. This timeline should include all affected systems and times of all activities and actions taken during the incident. Steps that victims and system administrators may have taken during the course of the incident, as well as in close proximity to the time range of the incident, are valuable items to document and discuss. Any deviation from organizational policy should be noted and taken as training items or assigned consequences in accordance with organizational policies. It may also be pertinent to ensure that appropriate information and intelligence sharing was performed during and after the incident occurred. Corrective actions that may have prevented the execution of malicious code, such as antivirus solutions, restrictions on where executables can run, tightened permissions, and script blockers for browsers, should be considered as a mitigation for the risks posed by malicious code threats. Web proxy blocks from information discovered during analysis can be utilized to ensure that malicious hosts are not contacted.

Ransomware execution

Post-incident activities for ransomware execution include all the activities involved with malicious code execution, with the addition of ensuring the functionality of a robust offline backup solution. An offline backup solution ensures that backup data is kept inaccessible to ransomware threats and is available if ransomware is successfully executed. A functional and frequent (such as daily incremental and weekly full) backup process helps ensure that business continuity is maintained in the event of issues and incidents.

Denial of service attack

Denial of service post-incident activities should include a timeline of traffic activities, as well as organizational responses to the attack traffic as well as the timeline of any business impacts and the damage associated with the impacts. Any attack precursors should be investigated and noted, and intelligence implemented to notify personnel and potentially take action as soon as attack traffic is observed. Impacts on affected systems should be noted, and a consensus should be reached on whether the systems should be upgraded or supplemented with load-balancing capabilities.

Social Engineering

Post-incident activities for social engineering incidents should include a timeline that includes all applicable activities, such as points of contact, narratives from the parties involved, CCTV footage (if applicable), system and network log files, and physical access control logging data. If unauthorized access was obtained, the impact of the access should be assessed and mitigating factors should be identified for inclusion to reduce the risk of future incidents (such as multifactor authentication, physical locks, greater CCTV coverage, improved physical access control, etc.). Security awareness training should be imperative if policy was breached, and information or access was given to unauthorized parties.

Phishing

Phishing post-incident activities should also include a timeline of actions taken since the phishing email was received, to include descriptions of the type of phishing campaign observed (malicious code, financial exploitation, credential harvesting, etc.), malicious attachments contained (if any), malicious or suspicious links in the body of emails, as well as narratives from recipients of the email and any potential victims, either self-reported or discovered through email, network, or host-based monitoring. If malicious code was included in the campaign, typical post-incident activities involving malicious code should be considered as well. Training opportunities can often arise from phishing attacks, whether successful or not, that can be valuable in giving employees better situational awareness regarding phishing.

The CJIS Security Policy requires each agency with access to CJI to establish operational incident handling procedures (i.e. a local policy). Gleaning from the requirements in Section 5.3 Incident Response, the local policy may include the following elements:

- Overall incident handling procedures. This section describes and identifies the processes used locally how the agency successfully prepares for, manages, and recovers from an incident. It includes sections on:
 - Preparation
 - Detection and Analysis
 - Containment

- Recovery
 - User response activities
- How the agency performs incident reporting. This section describes the process of notifying internal and external partners when an incident has occurred and how the incident is documented. It includes sections on:
 - Internal and external points of contact
 - Required tracking and reporting documents
 - Escalation procedures
- Incident management procedures. This section describes the agency's approach to a consistent and repeatable approach to managing incidents. It includes sections on:
 - Roles and responsibilities
 - Incident-related information collection
 - Updating policies with lessons learned
 - Collection of evidence
 - Incident response training
 - Document and artifact retention

G.8 Secure Coding

Secure Coding

This appendix documents a source of information on best practices and standards for secure coding. With the increased use of software products and the rapid pace of modern software development, it is essential to discover and resolve insecure software risks. The mitigations and guidelines to reduce these common risks can be found in secure coding best practices.

Understanding how software applications work can be a daunting thing; however, it could be key to know if data security is in jeopardy. Awareness of secure coding practices allows an agency to review potential vendors and their products prior to purchase and implementation. It also empowers the agency with the knowledge of the questions to ask a vendor of how the software was developed and whether the vendor uses secure coding practices or standards.

Additionally, the information in this appendix can provide a path forward for agencies with the internal capability to produce “in-house” software applications. By implementing security during the code writing process, security is “baked in” and there is more trust the software will aid in protecting the information it processes.

Open Web Application Security Project (OWASP) Foundation

The OWASP Foundation is a not-for-profit charitable organization focused on improving the security of software. OWASP operates as a community of like-minded professionals to provide unbiased and practical information about application security (AppSec) through software tools and documentation. These materials are available under a free and open software license, which can be located at the link below.

https://www.owasp.org/index.php/Main_Page

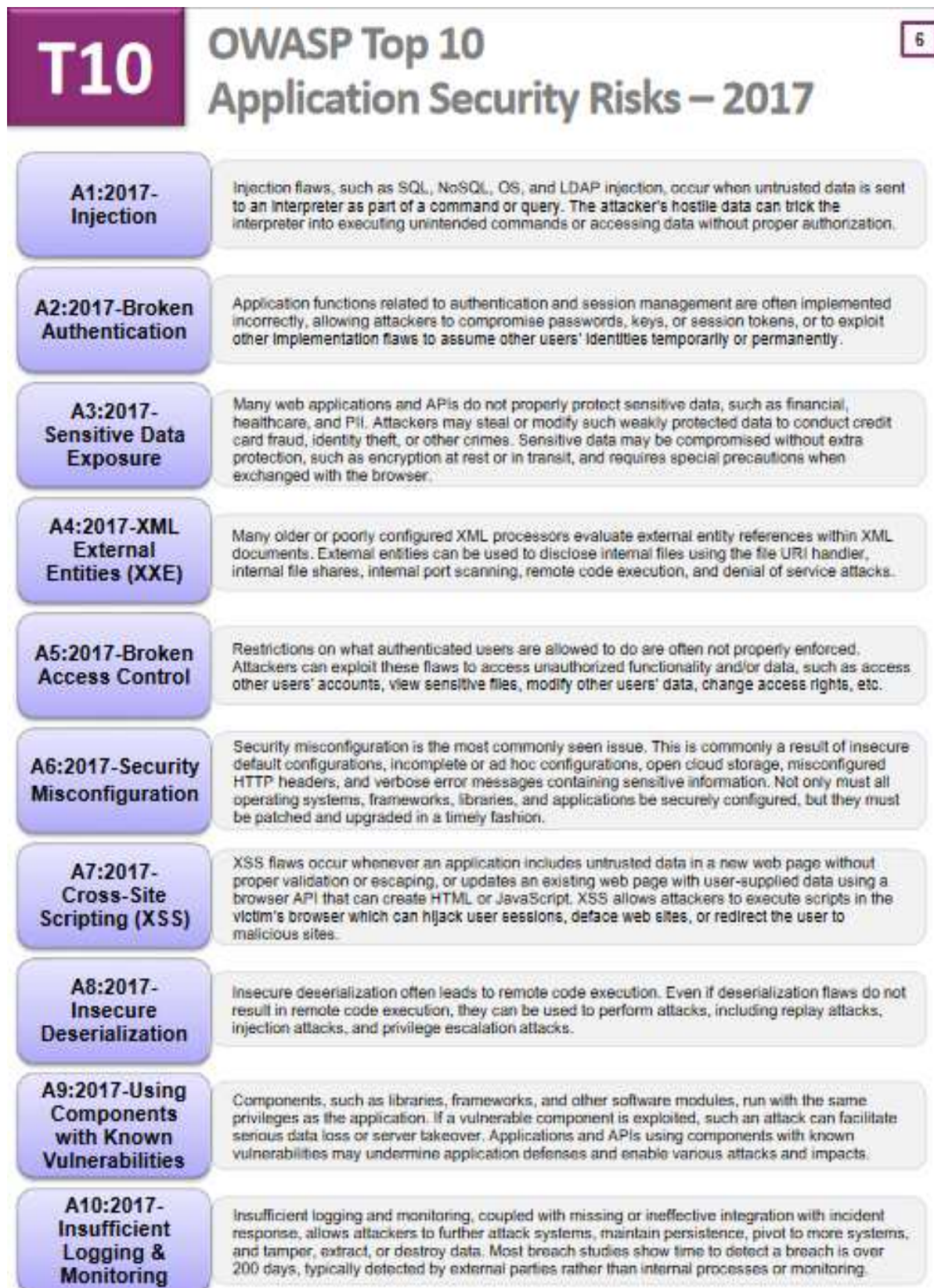
Software is becoming increasingly complex and connected, and the difficulty of achieving application security increases exponentially. The rapid pace of modern software development processes makes the most common risks essential to discover and resolve quickly and accurately.

The OWASP Foundation publishes the Top 10 Application Security Risks, which focus on the most serious web application security risks. The OWASP Top 10 is based primarily on 40 plus data submissions from firms that specialize in application security and an industry survey that was completed by over 500 individuals. This data spans vulnerabilities gathered from hundreds of organizations and over 100,000 real world applications and application program interfaces (API). The Top 10 items are selected and prioritized according to this data, in combination with consensus estimates of exploitability, detectability, and impact.

A primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risks problem areas, and provides guidance on a path forward.

The OWASP Top 10 focuses on identifying the most serious web application security risks for a broad array of organizations. For each of these risks, generic information about likelihood and technical impact using the following simple ratings scheme, which is based on the OWASP Risk Rating Methodology.

Figure G.8-A



Each organization is unique, and so are the threat actors for that organization, their goals, and the impact of any breach. It is critical to understand the risk to your organization based on applicable threat agents and business impacts.

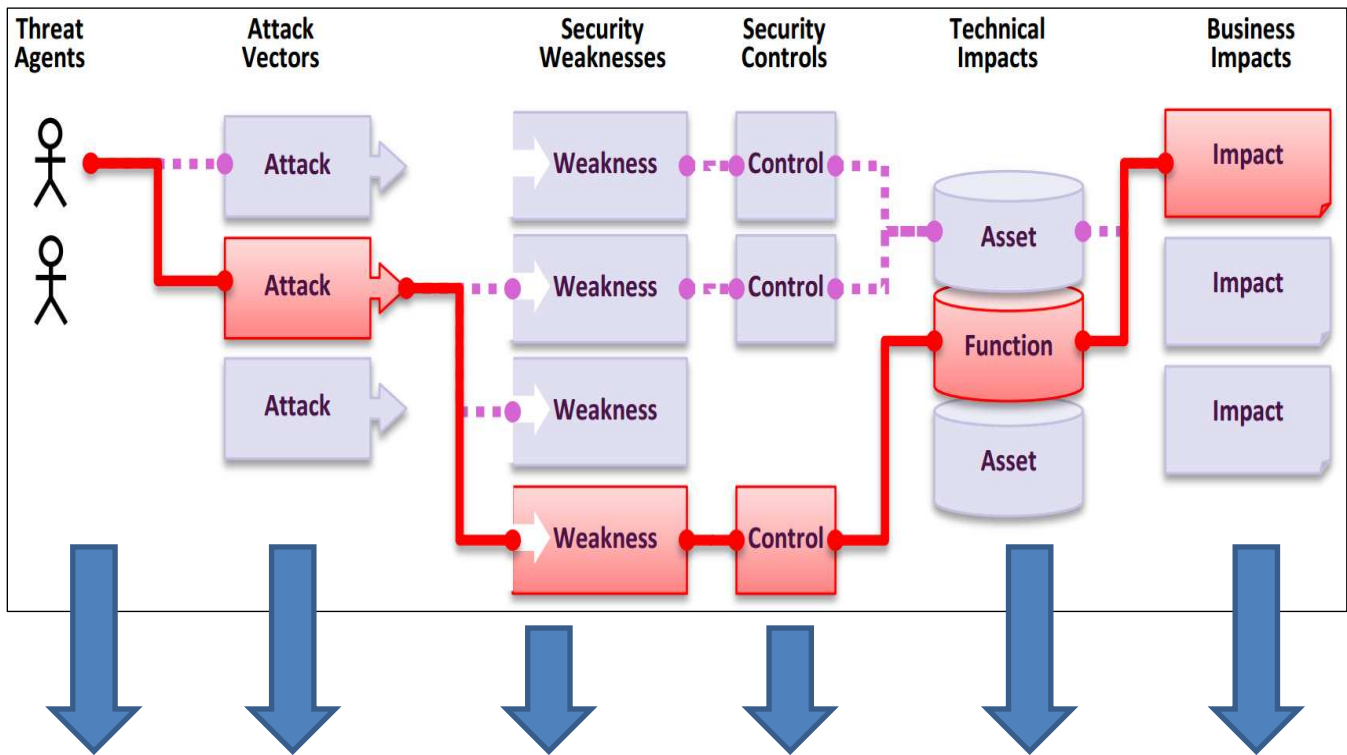
Application Security Risks

The figures immediately below illustrate the path of a sample threat beginning with the threat agent and ending with the target or affected business resource. Various paths are available but the agent would normally select the path of least resistance which would be the most vulnerable and with the fewest number of effective security controls.

The sample risk matrix can be used to assign in the various aspects of potential vulnerability. Each column corresponds to a phase in the attack process. In the matrix, a lower value represents less risk and is more desirable.

Concerning secure coding practices, when security is built-in during code development, vulnerabilities can be identified and controls included reducing the overall risk to information processed by the code.

Figure G.8-B Sample Threat Path



Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	SEVERE: 3	App / Business Specific
	AVERAGE: 2	COMMON: 2	AVERAGE: 2	MODERATE: 2	
	DIFFICULT: 1	UNCOMMON: 1	DIFFICULT: 1	MINOR: 1	

Figure G.8-C General Risk Matrix

To understand these risks for a particular application or organization, you must consider your own specific threat agents and business impacts. Even severe software weaknesses may not present a serious risk if there are no threat agents in a position to perform the necessary attack or the business impact is negligible for the assets involved. The following table presents a summary of the 2017 Top 10 Application Security Risks, and the risk factors that have been assigned to each risk.

Figure G.8-D Top 10 Risk Factor Summary

RISK							Score
	Threat Agents	Exploitability	Prevalence	Detectability	Technical	Business	
A1:2017-Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0
A2:2017-Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A3:2017-Sens. Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0

Whether you are new to web application security or already very familiar with these risks, the task of producing a secure web application or fixing an existing one can be difficult. If you have to manage a large application portfolio, this task can be daunting.

To help organizations, developers, testers and managers reduce their application security risks in a cost-effective manner; OWASP has produced numerous free and open resources that you can use to address application security in your organization. The following are some of the many resources OWASP has produced to help organizations produce secure web applications and APIs.

Get Started:

- Document all applications and associated data assets.
- Larger organizations should consider implementing a Configuration Management Database (CMDB).
- Establish an application security program to conduct analysis to define key improvement areas and an execution plan.

Risk Based Portfolio Approach:

- Identify the protection needs of your application portfolio from a business perspective.
- Establish a common risk-rating model with a consistent set of likelihood and impact factors reflective of your organization's tolerance for risk.
- Measure and prioritize all applications and APIs and add results to CMDB.

Enable with a Strong Foundation:

- Establish a set of policies and standards that provide an application security baseline for all development teams to adhere to.
- Define a common set of reusable security controls that complement these policies and standards and provide design and development guidance on their use.

Integrate Security into Existing Processes:

- Define and integrate secure implementation and verification activities into existing development and operational processes.
 - Activities include threat modeling, secure design and design review, secure coding and code review, penetration testing, and remediation.

Application Security Requirements - to produce a secure web application, you must define what secure means for that application.

- [Application Security Verification Standard \(ASVS\):](https://www.owasp.org/index.php/ASVS)
<https://www.owasp.org/index.php/ASVS>
- [OWASP Secure Software Contract Annex:](https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex)
https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

Application Security Architecture - retrofitting security into your applications and APIs, it is far more cost effective to design the security in from the start.

- OWASP Prevention Cheat Sheets:

https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series

Standard Security Controls - building strong and usable security controls is difficult. Using a set of standard security controls radically simplifies the development of secure applications and APIs.

- OWASP Proactive Controls:
https://www.owasp.org/index.php/OWASP_Proactive_Controls

Secure Development Lifecycle - to improve the process your organization follows when building applications and APIs, organizations formulate and implement a strategy for software security that is tailored to the specific risks facing their organization.

- OWASP Software Assurance Maturity Model (SAMM):
https://www.owasp.org/index.php/OWASP_SAMM_Project
- OWASP Application Security Guide for CISOs:
https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs

Application Security Education – hands-on learning about vulnerabilities to help educate developers on web application security.

- OWASP Education Project:
https://www.owasp.org/index.php/Category:OWASP_Education_Project
- OWASP WebGoat:
<https://www.owasp.org/index.php/WebGoat>
- OWASP Broken Web Application Project:
https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

Understand the Threat Model – be sure to understand the priorities when it comes to threat model.

- OWASP Testing Guide:
https://www.owasp.org/index.php/OWASP_Testing_Project
- [Application Security Verification Standard \(ASVS\):](https://www.owasp.org/index.php/ASVS)
<https://www.owasp.org/index.php/ASVS>

Testing Strategies – choose the simplest, fastest, most accurate technique to verify each requirement.

- OWASP Security Knowledge Framework:
https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework

- [Application Security Verification Standard \(ASVS\):
https://www.owasp.org/index.php/ASVS](https://www.owasp.org/index.php/ASVS)

APPENDIX H SECURITY ADDENDUM

The following pages contain the legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4); the Security Addendum itself (H5-H6); and the Security Addendum Certification page (H7).

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

**Legal Authority for and Purpose and Genesis of the
Security Addendum**

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security

addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

- a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
 - 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
 - 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
 - 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power

and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Printed Name/Signature of Contractor Employee

Date

Printed Name/Signature of Contractor Representative

Date

Organization and Title of Contractor Representative

APPENDIX I REFERENCES

White House Memo entitled “Designation and Sharing of Controlled Unclassified Information (CUI)”, May 9, 2008

[CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306

[CNSS Instruction No. 4009] *National Information Assurance (IA) Glossary*; Committee on National Security Systems (CNSS) Instruction No. 4009; 26 April 2010

[FBI SA 8/2006] *Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum*; 8/2006; Assistant Director, Criminal Justice Information Services, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306

[FISMA] *Federal Information Security Management Act of 2002*; House of Representatives Bill 2458, Title III–Information Security

[FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 199; February 2004

[FIPS 200] *Minimum Security Requirements for Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 200; March 2006

[FIPS 201] *Personal Identity Verification for Federal Employees and Contractors*; Federal Information Processing Standards Publication, FIPS PUB 201-1

[NIST SP 800–14] *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST Special Publication 800–14

[NIST SP 800–25] *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*; NIST Special Publication 800–25

[NIST SP 800–30] *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800–36

[NIST SP 800–32] *Introduction to Public Key Technology and the Federal PKI Infrastructure*; NIST Special Publication 800–32

[NIST SP 800–34] *Contingency Planning Guide for Information Technology Systems*; NIST Special Publication 800–34

[NIST SP 800–35] *Guide to Information Technology Security Services*; NIST Special Publication 800–35

[NIST SP 800–36] *Guide to Selecting Information Technology Security Products*; NIST Special Publication 800–36

[NIST SP 800–39] *Managing Risk from Information Systems, An Organizational Perspective*; NIST Special Publication 800–39

[NIST SP 800–40] *Procedures for Handling Security Patches*; NIST Special Publication 800–40

- [NIST SP 800–44] *Guidelines on Securing Public Web Servers*; NIST Special Publication 800–44
- [NIST SP 800–45] *Guidelines on Electronic Mail Security*; NIST Special Publication 800–45, Version 2
- [NIST SP 800–46] *Security for Telecommuting and Broadband Communications*; NIST Special Publication 800–46
- [NIST SP 800–48] *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*; NIST Special Publication 800–48
- [NIST SP 800–52] *Guidelines on the Selection and Use of Transport Layer Security*; NIST Special Publication 800–52
- [NIST SP 800–53] *Recommended Security Controls for Federal Information Systems*; NIST Special Publication 800–53, Revision 2
- [NIST SP 800–53A] *Guide for Assessing the Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*; NIST Special Publication 800–53A
- [NIST SP 800–58] *Security Considerations for Voice over IP Systems*; NIST Special Publication 800–58
- [NIST SP 800–60] *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800–60, Revision 1, DRAFT
- [NIST SP 800–63–1] *Electronic Authentication Guideline*; NIST Special Publication 800–63–1; DRAFT
- [NIST SP 800–64] NIST Special Publication 800–64
- [NIST SP 800–66] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA)*; NIST Special Publication 800–66
- [NIST SP 800–68] *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; NIST Special Publication 800–68
- [NIST SP 800–70] *Security Configuration Checklists Program for IT Products*; NIST Special Publication 800–70
- [NIST SP 800–72] *Guidelines on PDA Forensics*; NIST Special Publication 800–72
- [NIST SP 800–73] *Integrated Circuit Card for Personal Identification Verification*; NIST Special Publication 800–73; Revision 1
- [NIST SP 800–76] *Biometric Data Specification for Personal Identity Verification*; NIST Special Publication 800–76
- [NIST SP 800–77] *Guide to IPSec VPNs*; NIST Special Publication 800–77
- [NIST SP 800–78] *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; NIST Special Publication 800–78
- [NIST SP 800–81] *Secure Domain Name System (DNS) Deployment Guide*; NIST Special Publication 800–81
- [NIST SP 800–84] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*; NIST Special Publication 800–84

- [NIST SP 800–86] *Guide to Integrating Forensic Techniques into Incident Response*; NIST Special Publication 800–86
- [NIST SP 800–87] *Codes for the Identification of Federal and Federally Assisted Agencies*; NIST Special Publication 800–87
- [NIST SP 800–96] *PIV Card / Reader Interoperability Guidelines*; NIST Special Publication 800–96
- [NIST SP 800–97] *Guide to IEEE 802.11i: Robust Security Networks*; NIST Special Publication 800–97
- [NIST SP 800–121] *Guide to Bluetooth Security*, NIST Special Publication 800-121
- [NIST SP 800–124] *Guidelines on Cell Phone and PDA Security*, NIST Special Publication 800-124
- [NIST SP 800-125] *Guide to Security for Full Virtualization Technologies*; NIST Special Publication 800-125
- [NIST SP 800–144] *Guidelines on Security and Privacy in Public Cloud Computing*; NIST Special Publication 800-144
- [NIST SP 800–145] *The NIST Definition of Cloud Computing*; NIST Special Publication 800-145
- [NIST SP 800–146] *Cloud Computing Synopsis and Recommendations*; NIST Special Publication 800-146
- [OMB A–130] *Management of Federal Information Resources*; Circular No. A–130; Revised; February 8, 1996
- [OMB M–04–04] *E-Authentication Guidance for Federal Agencies*; OMB Memo 04–04; December 16, 2003
- [OMB M–06–15] *Safeguarding Personally Identifiable Information*; OMB Memo 06–15; May 22, 2006
- [OMB M–06–16] *Protection of Sensitive Agency Information*; OMB Memo 06–16; June 23, 2006
- [OMB M–06–19] *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; OMB Memo 06–19; July 12, 2006
- [OMB M–07–16] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Meme 07–16; May 22, 2007
- [Surviving Security] *Surviving Security: How to Integrate People, Process, and Technology*; Second Edition; 2004
- [USC Title 5, Section 552] *Public information; agency rules, opinions, orders, records, and proceedings*; United States Code, Title 5 - Government Agency and Employees, Part I - The Agencies Generally, Chapter 5 - Administrative Procedure, Subchapter II - Administrative Procedure, Section 552. Public information; agency rules, opinions, orders, records, and proceedings

[USC Title 44, Section 3506] *Federal Information Policy*; 01/02/2006; United States Code,
Title 44 - Public Printing and Documents; Chapter 35 - Coordination of
Federal Information Policy; Subchapter I - Federal Information Policy, Section
3506

APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Noncriminal Justice Agencies (NCJA) with access to Criminal Justice Information (CJI) as authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau (SIB) and/or Channeling agency. Examples of the target audience for the Appendix J supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to CJI maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those NCJAs new to the CSP and Advisory Policy Board (APB) auditing process (all NCJAs will be periodically audited by the CJIS Systems Agency (CSA)/SIB and may be included in a sampling of triennial audits conducted by the FBI) it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every NCJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific “shall” statement please go to the referenced section within the main body of the CSP.

General CJI Guidance

The following information provides NCJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. **3.2.9 – Local Agency Security Officer (LASO)**

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local NCJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and

procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.6 – Agency User Agreements

When an NCJA (private or public) is permitted to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions as authorized pursuant to federal law or state statute approved by the U.S. Attorney General, the information received from the background check, such as criminal history record information (CHRI) or personally identifiable information (PII), must be protected as CJI. In order to receive access to CJI the NCJA must enter into a signed written agreement, i.e., an agency user agreement, with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the CJI access. An example of a NCJA (private) is a local bank. An example of a NCJA (public) is a county school board.

Note 1: The CSA, SIB, or authorized agency providing the CJI access term should be part of the agency user agreement.

Note 2: Any NCJA that directly accesses FBI CJIS must allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2.1.1 – All Personnel (Security Awareness Training)

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

Note: The CSO/SIB may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help NCJAs with:

- (i) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,
- (ii) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative

to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient. The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to electronic and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

“Electronic media” is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store electronic and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn’t possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a criminal justice conveyance, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data “at rest”) of CJI.

i. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record

information for the purposes of licensing or employment need to follow the guidance in Section 5.12 (referenced below).

j. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Agencies located within states that have not passed legislation authorizing or requiring civil fingerprint-based background checks are exempted from this requirement until such time as appropriate legislation has been written into law.

The following scenarios are intended to help the reader identify areas within the CSP that NCJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above General CJI Guidance section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.

Hard Copy CJI Storage and Accessibility

When an NCJA receives CJI via a paper copy from a CJA and stores the paper within a locked file cabinet, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

Electronic CJI Storage and Accessibility – Controlled Area

When an NCJA creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control – Encryption

CSP Section 5.5.2.4 item 3 – Encryption describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this situation. Encrypted information can only be read by personnel possessing the

appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

Electronic CJI Storage and Accessibility – Physically Secure Location

When an NCJA receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy sections:

a. **5.5 – Access Control**

CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. **5.6 – Identification and Authentication**

CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. **5.7 – Configuration Management**

CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. **5.10 – System and Communications Protection and Information Integrity**

CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency's environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

Use Case Scenarios

1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that has indirect access to CJI and is located in a secure data center within the board of education offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to an employee's electronic record. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the record, the user is prompted to enter their unique username and password. Because the record resides on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required to access the record.

NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.

2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) encryption algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access an employee's record, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder.

NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.

APPENDIX K CRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Criminal Justice Agencies (CJA) that have historically not been subject to audit under the CJIS Security Policy guidelines. The target audience typically gains access to CJI via fax, hardcopy distribution or voice calls; does not have the capability to query state or national databases for criminal justice information; and may have been assigned an originating agency identifier (ORI) but is dependent on other agencies to run queries on their behalf. This guidance is not intended for criminal justice agencies covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CJIS Systems Agency (CSA) – in other words those agencies traditionally identified as “terminal agencies”.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to criminal justice information (CJI) maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those CJAs new to the CSP it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every CJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific “shall” statement please go to the referenced section within the main body of the CSP.

General CJI Guidance

The following information provides CJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. 3.2.9 – Local Agency Security Officer (LASO)

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local CJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.3 – Criminal Justice Agency User Agreements

Any CJA receiving access to CJI must enter into a signed agreement with the CSA providing the access. The agreement specifies the services and systems the agency will access. It must also specify all pertinent governance policies to which the agency must adhere.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2 – Security Awareness Training

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

CSP Section 5.2.1.2 describes the topics required to be discussed for personnel that have both physical and logical access to CJI. These topics are covered in addition to the ones addressed in basic security awareness training.

CSP Section 5.2.1.3 describes topics to be covered for those personnel assigned information technology roles. Topics covered in this section are in addition to the topics addressed in Sections 5.2.1.1 and 5.2.1.2.

Note: The CSO may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help CJAs with:

- (iii) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,
- (iv) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient.

The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to digital and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

“Digital media” is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store digital and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn’t possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy digital media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a police vehicle, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data “at rest”) of CJI.

i. 5.10 – System and Communications Protection and Information Integrity

CSP Section 5.10 explains the technical safeguards ranging from boundary and transmission protection to security an agency’s virtualized environment.

CSP Section 5.10.1.2 details the requirements for the encryption of CJI whether in transit or at rest. FIPS 140-2 certification is required when CJI is in transit outside a physically secure location. When at rest outside a physically secure location, encryption methods can use Advanced Encryption Standard (AES) at 256 bit strength or a FIPS 140-2 certified method.

CSP Section 5.10.3 explains the use of virtualization and partitioning when processing CJI in a virtual environment. A virtualized environment can be configured such that those parts of the system which process CJI are either physically or virtually separated from those that do not.

CSP Section 5.10.4 explains system and information integrity policy and procedures. This includes areas such as patch management, malicious code protection, and spam and spyware protection.

j. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one

representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

k. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

l. 5.13 – Mobile Devices

When access to CJI using mobile devices such as laptops, smartphones, and tablets is authorized, CSP Section 5.13 explains the controls required to manage those devices to ensure the information remains protected.

The following scenarios are intended to help the reader identify areas within the CSP that CJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above “General CJI Guidance” section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.

Hard Copy CJI Storage and Accessibility

When CJI is received in hard copy and the agency stores the paper within a locked file cabinet, the CJA should, in addition to the “General CJI Guidance”, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

Electronic CJI Storage and Accessibility – Controlled Area

When an agency creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the agency should, in addition to the “General CJI Guidance”, focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control Mechanisms – Encryption

CSP Section 5.5.2.4 item 3, Encryption – This describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this

situation. Encrypted information can only be read by personnel possessing the appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

Electronic CJI Storage and Accessibility – Physically Secure Location

When an agency receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the agency should, in addition to the “General CJI Guidance”, focus on compliance with policy sections:

a. **5.5 – Access Control**

CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. **5.6 – Identification and Authentication**

CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. **5.7 – Configuration Management**

CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. **5.10 – System and Communications Protection and Information Integrity**

CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency’s environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

Use Case Scenarios

1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

A county court scans hard copy case documents containing CJI into an electronic format. The documents are placed on a network server which is located in a secure data center within the court offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to case documents. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the documents, the user is prompted to enter their unique username and password. Because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.

2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

A county court scans hard copy case documents containing CJI in an electronic format. The documents are placed on a network server which is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access to the case documents, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder. Additionally, because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.

Utah 41-6a-1803 effective May 2024.pdf

Effective 5/1/2024

41-6a-1803 Driver and passengers -- Seat belt or child restraint device required.

- (1)
- (a) Except as provided in Subsection (1)(c), the operator of a motor vehicle operated on a highway shall:
 - (i) wear a properly adjusted and fastened safety belt;
 - (ii) provide for the protection of each person younger than eight years old by using a child restraint device to restrain each person in the manner prescribed by the manufacturer of the device; and
 - (iii) provide for the protection of each person that is at least eight years old and no less than 16 years old by securing, or causing to be secured, a properly adjusted and fastened safety belt on each person.
 - (b) Notwithstanding the requirement under Subsection (1)(a)(ii), a child under eight years old who is 57 inches tall or taller:
 - (i) is exempt from the requirement in Subsection (1)(a)(ii) to be in a child restraint device; and
 - (ii) shall use a properly adjusted and fastened safety belt as required in Subsection (1)(a)(iii).
 - (c) An adult passenger who is utilizing transportation network services described in Section 13-51-102 or a taxicab described in Section 53-3-102 shall:
 - (i) provide for the protection of each person younger than eight years old who is under the adult's supervision by using a child restraint device to restrain the person in the manner prescribed by the manufacturer of the device; and
 - (ii) provide for the protection of each person who is under the adult's supervision and is at least eight years old and no less than 16 years old by securing, or causing to be secured, a properly adjusted and fastened safety belt on the person.
- (2) A person 16 years old or older who is a passenger in a motor vehicle operated on a highway shall wear a properly adjusted and fastened safety belt.
- (3) If more than one person is not using a child restraint device or wearing a safety belt in violation of Subsection (1), it is considered only one offense, and the driver may receive only one citation for that offense.

Amended by Chapter 351, 2024 General Session

Outside Employment Form.pdf



SOUTH SALT LAKE POLICE DEPARTMENT

REQUEST FOR OUTSIDE EMPLOYMENT

Name: _____ Date Submitted: _____

OFF DUTY EMPLOYER INFORMATION

Name of Employer: _____ Address: _____

Phone Number: _____ Immediate Supervisor: _____

Job Title: _____ Specific Duties: _____

Number of days per week expected to work: _____ Hours expected to work each day: _____

Can the work be canceled temporarily if you are called out to an emergency? _____

Date this employment will terminate: _____

_____ I certify that I have read and understand the South Salt Lake Police Department policy and procedure pertaining to Fitness for Duty and agree to follow all applicable policies. Date _____

_____ I certify that I have read and understand the South Salt Lake Police Department policy and procedure pertaining to Outside Employment and agree to follow all applicable policies. Date _____

_____ I certify that I have read and understand the South Salt Lake Police Department policy and procedure pertaining to Vehicle Policy and agree to follow all applicable policies. Date _____

I understand that if I deviate from this policy I may be subject to disciplinary action.

_____ I agree to notify the department in writing of any changes in the above information.

*All acknowledged policies are attached to this request

Approved: _____ Disapproved: _____

Officer's Signature / DP# Date

Approved: _____ Disapproved: _____

Sergeant's Signature / DP# Date

Division Commander Signature / DP# Date

Chief's Signature Date

Subject to the following conditions: _____

OFF DUTY EMPLOYMENT LAW ENFORCEMENT RELATED

All officers working off duty law enforcement related employment within the City of South Salt Lake should be aware that they continue to be governed by the policies and procedures, Professional Standards and Conduct Manual of the City of South Salt Lake, the South Salt Lake Police Department as well as any standard operating procedures set forth by the Chief of Police or his designee. BWC shall be worn and activated per SSLPD Policy in all off-duty law enforcement related employment.

Expiration Date: _____ (All off duty law enforcement employment is subject to review annually or at the appointment of a new police chief)

Light Duty Form.pdf



DANIELLE CROYLE
CHIEF OF POLICE

2835 S MAIN ST
SOUTH SALT LAKE CITY
UTAH
84115
O 801.412.3609
F 801.412.3620
TTY: 711
SSLC.GOV



CHERIE WOOD
MAYOR

220 E MORRIS AVE
SUITE 200
SOUTH SALT LAKE CITY
UTAH
84115
O 801.464.6757
F 801.464.6770

Temporary Modified-Duty Assignment Position or Light Duty Form

Employee Information:

Name: _____

Position: Desk Officer (Modified Duty)

Assignment: _____

Supervisor: _____

Light Duty Assignment:

Effective Dates: From _____ to _____

Work Schedule:

Days: Monday through Friday

Hours:

Location: Front Desk at Police Department

Responsibilities and Expectations:

Greeting Visitors:

Welcome and assist visitors and clients in a professional and courteous manner.

Assist community members who walk into the department and provide information over the telephone.

Answering Phones:

Answer incoming calls promptly and direct them to the appropriate person or department.

Take and relay messages accurately.

Compliance and Safety:

Adhere to all policies and procedures.

Ensure safety protocols are followed, including emergency procedures.

Desk Officer/Modified Duty:

The desk officer/modified duty position is a fixed post at the police department.

The assignment may be made as the needs of the department require.

The assignment may be for an entire shift or portion of that shift as determined by the shift supervisor.

Officer Response Coordination:

Forward information to VECC when an officer's response to the scene is appropriate.

If the caller is unwilling to provide report details over the phone or respond to the office, refer incidents to the shift supervisor

Report Handling:

Take reports via telephone or in person that do not require on-scene action, such as collection of evidence, photographs, or follow-up.

Notify the on-duty supervisor of the need for a patrol officer is needed on a scene or at the front desk, as soon as practical

Complete supplemental reports to any original report as required.

Ensure all reports are completed by the end of the shift, prior to going off duty. If an exception is needed, get approval from the shift supervisor.

Other Duties:

Perform other duties based on capabilities as assigned by shift supervisor.

Restrictions:

Employee on light duty due to medical or other reasons. Physical activities should be limited to ensure compliance with medical recommendations.

Additional Notes:

Acknowledgement:

I acknowledge that I have read and understand the responsibilities and expectations outlined in this Light Duty Form.

Employee Signature: _____ Date: _____

Supervisor Signature: _____ Date: _____

South Salt Lake PD Policy Manual

South Salt Lake PD Policy Manual

INDEX / TOPICS

A

ADMINISTRATIVE INVESTIGATIONS

OIS. 120

ADULT ABUSE

Investigations. 461

AIRCRAFT. 321

Ambulance. 403

AIRCRAFT ACCIDENTS. 321

ALCOHOL. 704

ALCOHOL

Intoxicants. 50

ALCOHOL USE. 704

ANIMALS

Line-of-duty death. 811

APPOINTMENTS

Audio/video coordinator. 352

Community relations coordinator. 232

Operations director. 511

Petty cash fund manager. 560

ARRESTS

Authority. 10

Child and dependent adult safety. 221

Consular Notifications. 635

Domestic violence. 108

First amendment assemblies. 410

ASSET FORFEITURE. 471

AUDIO/VIDEO RECORDING

Custodial interrogation. 460

AUDITS

Informant files. 481

Petty cash. 560

Public safety video surveillance. 209

AUTHORITY. 10

Canine handler. 275

B

BADGE

Mourning Badge. 760

BADGES, PATCHES AND IDENTIFICATION

Conduct. 47

BARRICADED SUSPECTS. 296

BATON. 79

BIOLOGICAL SAMPLES

Hazards. 322

BODY ARMOR. 728

BODY ARMOR

Suspects. 97

BOMBS. 301

Aircraft accidents. 322

Portable audio/video recorders. 351

BREATH TESTS. 440

C

CANINE

Handler Compensation. 277

CANINES

Pursuits. 358

CASH

Audit. 484

Informants. 483

CASH. 560

CHANGE OF ASSIGNMENT. 734

CHIEF EXECUTIVE OFFICER. 13

CHILD ABUSE. 161

CHILD AND DEPENDENT ADULT SAFETY 221

CHILDREN

Child safety. 221

Drug endangered. 164

Transporting. 726

CITE AND RELEASE. 309

CIVIL

Subpoenas. 177

CIVIL DISPUTES. 390

COMMAND STAFF

Work-related injuries and illnesses. 753

COMMENDATIONS AND AWARDS. 736

COMMUNICABLE DISEASES. 709

COMMUNICATIONS CENTER

Foot pursuits. 361

Mandatory sharing. 189

COMMUNITY ADVISORY COMMITTEE. 235

COMMUNITY RELATIONS. 232

COMPUTERS

Digital evidence. 461

CONDUCT. 44

Meritorious. 737

Standards of conduct. 49

CONFIDENTIALITY

Conduct. 47

Informants. 479

Surreptitious recording. 350

CONSTITUTIONAL REQUIREMENTS. 11

CONTACTS AND TEMPORARY DETENTIONS

Bias-based policing. 53

South Salt Lake Police Department

South Salt Lake PD Policy Manual

South Salt Lake PD Policy Manual

CONTROL DEVICES.	78
CONTROL DEVICES.	78
CONTROL DEVICES	
Training.	312
CORRESPONDENCE.	36
COURT ORDERS	
Adult abuse.	138
Child custody.	222
Civil disputes.	390
Foreign.	110
Subpoenas.	176
Surreptitious recording.	350
CRIME SCENE AND DISASTER	
INTEGRITY.	283
CRIMINAL OFFENDER INFORMATION.	599
CRISIS INTERVENTION INCIDENTS. . .	396
CRISIS NEGOTIATION TEAM.	285
CRISIS RESPONSE UNIT.	285
CUSTODIAL INTERROGATIONS. . . .	460

D

DAMAGE BY CITY PERSONNEL. . . .	169
DEATH	
Custody.	638
DEATH NOTIFICATION.	196
DEBRIEFING	
OIS.	121
Operation plans.	514
DEFECTIVE VEHICLES.	542
DEPENDENT ADULTS	
Safety.	221
DISABLED	
Motorist.	447
DISCLAIMER OF POLICIES.	14
DOG BITES.	273
DOG INJURIES.	273
DRIVING	
MDT/MDC.	347
Safety.	50
DRUG USE.	704

E

ELDER ABUSE.	135
ELECTRICAL LINES.	320
ELECTRONIC CIGARETTES.	714
EMERGENCY UTILITY.	320
EVIDENCE	
Bombs.	305
Digital.	461
Personnel complaints.	717

Public safety video surveillance.	209
Seizing recordings.	394
EXPLOSIONS.	304
EXPOSURE CONTROL.	709
EXPOSURES.	293

F

FIELD IDENTIFICATION.	487
FIELD TRAINING OFFICER.	325
FIELS SOBRIETY TESTS.	439
FIREARMS	
Conduct.	50
Retiree carry.	40
FIREARM SERIAL NUMBERS.	592
FIRST AMENDMENT ASSEMBLIES. . .	406
FOREIGN	
Court orders.	110
Nationals.	635
FORMS	
Child abuse and narcotics.	165

G

GANGS	
Employee affiliation.	46
GENERAL ORDER.	39
GROOMING STANDARDS.	755

H

HATE CRIMES.	128
HAZARDOUS MATERIAL (HAZMAT)	
RESPONSE	
Aircraft accidents.	322
HAZARDOUS MATERIALS RESPONSE. .	293
HAZMAT.	293
HELICOPTER ASSISTANCE.	328
HOSTAGE AND BARRICADE INCIDENTS	
Rapid response and deployment.	312
HOSTAGES.	296

I

INFORMANTS.	479
INTERNAL AFFAIRS	
Personnel records.	732
INVESTIGATION AND PROSECUTION. .	459

J

JURISDICTION	
Aircraft accidents.	322
Authority.	10

South Salt Lake Police Department

South Salt Lake PD Policy Manual

South Salt Lake PD Policy Manual

Consular Notification.	635
Foreign court orders.	110
OIS.	114

K

KINETIC PROJECTILES.	82

L

LAW ENFORCEMENT AUTHORITY.	10
LEG RESTRAINT.	93
LIMITED ENGLISH PROFICIENCY.	198
LIVE LINEUP.	487

M

MANDATORY EMPLOYER NOTIFICATION	206
MEAL PERIODS AND BREAKS.	741
MEDIA	
Aircraft accidents.	323
First amendment assemblies.	410
OIS.	122
Operations plans.	514
Warrant service.	519
MEDIA RELATIONS.	171
MEDICAL	
Aircraft accidents.	321
Child involuntary detention.	164
Examinations - adult abuse.	140
Examinations - Child abuse.	164
Leave Act (FMLA).	707
Personnel Records.	732
Releases.	403
Treatment for work-related injury or illness	753
MENTAL ILLNESS	
Restraints.	306
MISSING PERSON.	143
MOBILE AUDIO VIDEO.	339
MODIFIED-DUTY ASSIGNMENTS.	768
MUTUAL AID	
Interstate peace officer powers.	12

N

NARCOTIC-DETECTION DOGS.	272
NONSWORN	
Crisis intervention incidents.	399
NOTIFICATION	
Consular.	635
NOTIFICATIONS	
Aircraft accidents.	322
Cash.	561

Custody suicide attempt, death or serious injury.	638
Mandatory employer.	206
OIS.	116
Sick leave.	707

O

OATH OF OFFICE.	20
OCCUPATIONAL DISEASE AND WORK-RELATED INJURY AND DEATH REPORTING.	753
OC SPRAY.	81
OFFICER-INVOLVED SHOOTING	
OIS.	114
OFFICER SAFETY	
Domestic violence.	106
Firearm confiscation.	116
Foot pursuits.	358
Informants.	480
LEOSA.	40
Portable audio/video recorders.	348
Seat belts.	726
Warrant service.	515
OPERATIONS PLANNING AND DECONFLICTION.	511
OUTSIDE AGENCY ASSISTANCE.	188
OUTSIDE EMPLOYMENT.	749
Obtaining Approval.	749
Prohibited Outside Employment.	750
Security Employment.	751
OVERTIME	
Court.	178

P

PATROL FUNCTION.	266
PAWN SHOP HOLDS.	496
PEPPER PROJECTILES.	81
PERFORMANCE EVALUATIONS	
Sick leave.	708
PERSONAL APPEARANCE.	755
PERSONNEL RECORDS.	730
PHOTOGRAPHIC LINEUP.	487
PHOTOGRAPHS	
Aircraft accidents.	323
PHYSICAL AND MENTAL EXAMINATIONS.	739
POLICY MANUAL.	14
PRIVACY EXPECTATIONS	
Audio/Video recordings.	348
PROPERTY PROCEDURES	

South Salt Lake Police Department

South Salt Lake PD Policy Manual

South Salt Lake PD Policy Manual

Property Booking.	568
PROTECTED INFORMATION.	599
PROTECTED INFORMATION	
Unauthorized release.	47
PROTECTIVE CUSTODY	
Dependent adults.	138
PUBLIC RECORDING OF LAW	
ENFORCEMENT ACTIVITY.	393
PUBLIC SAFETY VIDEO SURVEILLANCE	
VIDEO RECORDING	
Audio/Video.	207
PURSUIITS	
Foot.	358

R

RAPE KITS.	467
RAPID RESPONSE AND DEPLOYMENT.	311
RECORDS	
Suspicious activity reports.	413
RECORDS BUREAU	
Administrative hearings.	444
Impaired driving.	444
RECORDS RELEASE	
Adult abuse.	141
Audio/video recordings.	353
Personnel records.	733
Public safety video surveillance.	209
RECORDS REQUESTS	
Personnel records.	733
RECORDS RETENTION	
Audio/video recordings.	351, 353
Oath of office.	21
Personnel records.	732
RECRUITMENT AND SELECTION.	690
REPORT PREPARATION.	167
Report corrections.	170
RESERVE OFFICERS	
Auxiliary Officers.	179
Firearms Requirements.	184
RESPONSE TO CALLS.	56
RESTRAINTS.	93
REVIEWS	
Crisis intervention incidents.	399
RIDE-ALONG.	290

S

SAFETY	
Conduct.	50
SAFETY EQUIPMENT	
Seat belts.	726
SEARCH WARRANTS.	516

SECURITY	
Personnel records.	733
SECURITY EMPLOYMEN.	751
SICK LEAVE.	707
SMOKING AND TOBACCO USE.	714
SPIT HOOD.	94
SPIT MASK.	94
STAFF.	14
STANDARDS OF CONDUCT.	44
SUBPOENAS.	176
SUBPOENAS AND COURT APPEARANCES	176
SURVEILLANCE	
Imaging notification.	518
SUSPICIOUS ACTIVITY REPORTING.	412

T

TATTOOS.	756
TEAR GAS.	79
TRAINING.	603
TRAINING	
Adult abuse.	141
Child and dependent adult safety.	224
Communicable disease.	712
Community Development.	236
Crisis intervention incidents.	400
Custody.	639
Fair and objective policing.	54
Firearms.	102
First amendment assemblies.	411
Operation planning and deconfliction.	514
Personnel records.	731
Public safety video surveillance.	210
Rapid response and deployment.	312
Records maintenance and release.	598

U

UNIFORM REGULATIONS.	757
UNIFORMS	
Courtroom attire.	177
URINE TESTS.	440
UTILITY SERVICE.	320

V

VEHICLE MAINTENANCE.	542

W

WARRANT SERVICE.	515
WATCH COMMANDERS.	337
WATER LINES.	320