



# TALLAHASSEE POLICE DEPARTMENT GENERAL ORDERS

 Proudly Policing Since 1841	<b>SUBJECT</b> Computer, Cellular Telephone and Data Utilization		 Nationally Accredited 1986
	<b>CHIEF OF POLICE</b> <i>Signature on File</i>		
<b>NUMBER</b> 77	<b>ORIGINAL ISSUE</b> 06/18/2014	<b>CURRENT REVISION</b> 07/16/2021	<b>TOTAL PAGES</b> 39

## AUTHORITY/RELATED REFERENCES

28 U.S. Code § 534, Acquisition, Preservation, and Exchange ... and Information  
 28 Code of Federal Regulations, Part 20, Criminal Justice Information Systems  
 COT Administrative Policy 405, Computer Security Incident Response  
 COT Administrative Policy 706, Working Conditions  
 COT Administrative Policy 809, Information Systems Security Procedures  
 FBI CJIS Security Policy  
 Florida Administrative Code 11C-6, Criminal History Records Dissemination Policy  
 Florida General Records Schedule GS-2  
 FS Chapter 119, Public Records  
 FS 381.987, Public Records Exemption ... Information Relating to Medical Marijuana ...  
 FDLE Guidelines for CJIS Access  
 General Order 12, Radio Communications  
 General Order 16, Digital Audio and Video Recording System  
 General Order 17, Records Management  
 General Order 18, Criminal Investigations  
 General Order 19, Digital Evidence Capturing Devices  
 General Order 20, Corrective Action Procedures  
 General Order 46, Rules of Conduct  
 General Order 55, Rapid ID Devices  
 Special Order 10, Building Security and Evacuation  
 Training Bulletin 13-02 DAVID Modernization Project

## ACCREDITATION REFERENCES

CALEA Chapters    11, 41  
 CFA Chapter        26

## KEY WORD INDEX

**Account Management**  
**Audits and Inspections**

Appendix One  
 Procedure XV

## TALLAHASSEE POLICE DEPARTMENT

---

<b>Background Checks</b>	Procedure XVII
<b>Cellular Telephone – Issuance/Activation</b>	Procedure VIII
<b>Cellular Telephone – Member Responsibilities</b>	Procedure IX
<b>CJIS Security Protocols – Department</b>	Procedure XI B
<b>CJIS Security Protocols – FAC</b>	Procedure XI E
<b>CJIS Security Protocols – Members</b>	Procedure XI D
<b>CJIS Security Protocols – T&amp;I Employees</b>	Procedure XI C
<b>CJIS Validations</b>	Procedure XIV
<b>CrimeView Protocols</b>	Procedure XVIII
<b>E-mail Protocols</b>	Procedure VI
<b>General Information</b>	Procedure I
<b>Internet Use</b>	Procedure VII
<b>Maintenance of Department-issued Computers</b>	Procedure IV
<b>Media Disposal Protocols</b>	Procedure XIII
<b>Member Responsibilities – General</b>	Procedure II
<b>Member Responsibilities – In-car MDC</b>	Procedure III
<b>Retention and Dissemination Protocols</b>	Procedure XII
<b>Telecommunications Applications Protocols</b>	Procedure X
<b>Utilization of Personally Owned Devices</b>	Procedure V
<b>Violations and Sanctions</b>	Procedure XVI

### **POLICY**

The Department will establish computer, cellular telephone and data utilization protocols for conducting Department business, providing best practices in access, security of equipment and data, information retention and dissemination of records. Members shall adhere to established Department protocols when operating City of Tallahassee computer equipment, cellular telephones, and processing public safety information.

### **DEFINITIONS**

**AVR:** Digital Audio and Video Recording System.

**CJIS:** Florida's Criminal Justice Information Services.

**Criminal Justice Information:** Public safety information provided to the Department via repositories maintained by the Federal Bureau of Investigation (FBI), the Florida Department of Law Enforcement (FDLE), and the Florida Department of Highway Safety and Motor Vehicles (DHSMV) or other computer interfaces via the Florida Criminal Justice Network (e.g., NCIC, FCIC, CJIS, DAVID, ELVIS, eAgent). Criminal justice information contains personally identifiable information (PII).

**DAVID:** Driver and Vehicle Information Database.

## TALLAHASSEE POLICE DEPARTMENT

---

**Department-issued Computer:** Any Department-issued desktop or mobile data computer (MDC) provided to a member as part of their work assignment, including those supplied on a temporary basis.

**ELVIS:** Electronic License and Vehicle Information System.

**FCIC:** Florida Crime Information Center.

**In-car MDC:** A mobile data computer designed to be docked in a mount inside a Department vehicle (e.g., MDC issued to officers in the Patrol Operations Bureau).

**LASO:** Local Agency Security Officer. A COT Technology & Innovations employee assigned to the Department who serves as the primary contact between the Department and the FDLE regarding the security of criminal justice information accessed via the COT computer network.

**MDC Hotline:** Telephone number to report MDC operating problems (891-4051).

**MDC Unit:** A work unit within the COT Technology & Innovations Department responsible for MDC administration and maintenance.

**Misuse:** Unauthorized use which includes, but is not limited to, queries unrelated to the administration of criminal justice or an authorized noncriminal justice purpose (e.g., employment background check), any personal use, and the dissemination, sharing or passing along of criminal justice information or personally identifiable information to any unauthorized person.

**MMUR:** Medical Marijuana Use Registry, hosted by Florida Department of Health.

**NCIC:** National Crime Information Center.

**Personally Identifiable Information (PII):** Data which alone can be used to distinguish or trace a person's identity or, when combined with other personal or identifying information which is linked or linkable to a specific person, can distinguish or trace a person's identity. PII can be extracted from CJI. See subsection XI B 11 below for examples of PII.

**Physically Secure Location:** A designated area with both the physical and personnel security controls sufficient to protect criminal justice information and associated information systems.

**Public Record:** All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other materials, regardless of physical form, characteristics, or means of transmission, made or received pursuant to law, ordinance, or in connection with the transaction of official business.

## TALLAHASSEE POLICE DEPARTMENT

---

**Public Safety Information:** Any public record related to the business of the Department in the fulfillment of its mission to protect and enhance the quality of life for our citizens. Criminal justice information and personally identifiable information are examples of public safety information.

**RSA Device:** An advanced authentication mechanism (e.g., key fob) which generates a unique authentication code at fixed intervals. The code, coupled with the member's User ID and password, allows access to the COT computer network via the MDC (mobile data computer).

**Security Alerts and Advisories:** Communications from governmental entities or private vendors about cyber security. *Alerts* provide timely notification to critical infrastructure owners and operators concerning threats to critical infrastructure networks. *Advisories* provide timely information about current security issues, vulnerabilities and exploits.

**Security Breach Incident:** An intentional or accidental situation which results (or potentially results) in the unauthorized dissemination of criminal justice information involving electronic systems (e.g., desktops, smartphones, mobile data computers, tablets) and/or physical documents (i.e., print-outs).

**Telecommunications Application:** A software application or computer program which facilitates voice, video and/or text communications between two or more persons. Such applications include Microsoft Skype, Microsoft Teams, Google Duo, and Apple FaceTime. For the purposes of this policy, telecommunications applications do not include the default/built-in voice calling or text messaging applications on Department-issued cellular phones.

**TraCS:** Traffic and Criminal Software.

**User ID:** The City-issued moniker facilitating access to the COT computer network.

## PROCEDURES

### I. GENERAL INFORMATION

- A. City of Tallahassee (COT) computers, cellular telephones, related equipment and software are provided to members for Department business in the fulfillment of its mission.
- B. COT computers and cellular telephones, and all information received on, transmitted through, or stored on or through a Department-issued computer or cellular telephone is the property of the COT.

## TALLAHASSEE POLICE DEPARTMENT

---

- C. Members do not have a right to privacy in the utilization of a Department-issued computer or cellular telephone, or the COT computer network. Nor do members have an expectation of privacy for the information contained on the computer or cellular telephone.
- D. All public safety information is subject to inspection and/or copying pursuant to FS Chapter 119, Public Records.
- E. In response to a public records request involving a Department-issued computer or cellular telephone, the COT will provide all texts, e-mails, and call logs connected to the telephone, except information legally exempt from release.
- F. Members who have a proposal for new software applications and/or phone settings for the Department-issued cellular telephones should forward the information to their chain of command via e-mail and courtesy copy the MDC Unit at [tpdmdc@talgov.com](mailto:tpdmdc@talgov.com) ("TPD MDC").
- G. Violations of this written directive subject a member to progressive discipline as set forth in General Order 20 (Corrective Action Procedures).

### **II. MEMBER RESPONSIBILITIES – GENERAL**

- A. Members are responsible for utilizing Department-issued computers and cellular telephones in a lawful, professional and ethical manner.
- B. Members shall utilize Department-issued computers and cellular telephones for Department business only.
- C. In their use of a Department-issued computer or cellular telephone, members are responsible for adhering to any related Department-provided training, orientation and familiarization.
- D. Members are prohibited from sending or forwarding offensive, threatening, harassing, slandering, obscene/suggestive, defamatory, sexual or otherwise inappropriate material or comments on a Department-issued computer or cellular telephone.
- E. In their use of a Department-issued computer or cellular telephone, members are responsible for adhering to the mandates of General Order 46 (Rules of Conduct) regarding:
  - 1. Performance of duties,
  - 2. Conduct toward others,

## TALLAHASSEE POLICE DEPARTMENT

---

3. Maintaining Department property, equipment and facilities, and
  4. For a cellular telephone, verbal identification over the telephone.
- F. Members are not authorized to make or direct software modifications to a Department-issued computer or cellular telephone without specific Department approval.

### III. MEMBER RESPONSIBILITIES – IN-CAR MDC

- A. Members with an in-car MDC shall have it logged on during the time frame in which a member is operating a Department-owned vehicle from the point the member enters the vehicle, without interruption, until the member exits the vehicle upon the conclusion of their shift or other work related activity (e.g., special event, secondary employment).
- B. Members driving a vehicle shall not operate the in-car MDC while the vehicle is in motion other than to indicate a response to a call for service (i.e., accept the call, en route, arrived).
- C. At the conclusion of their shift or other work-related activity (e.g., special event, secondary employment), members shall log off the MDC and shut down the computer in the manner prescribed in MDC training.
- D. Each in-car MDC has an Automatic Vehicle Locator (AVL) system, and members shall:
  1. Not tamper with the AVL system, to include the global positioning system receiver, antenna, wiring or software or attempt to hinder the system's designed performance, and
  2. Promptly report problems with the AVL system to their immediate supervisor and the MDC Unit via the MDC Hotline or e-mail at [tpdmdc@talgov.com](mailto:tpdmdc@talgov.com) ("TPD MDC").

### IV. MAINTENANCE OF DEPARTMENT-ISSUED COMPUTERS

- A. In addition to the Maintaining Department Property, Equipment and Facilities protocols of General Order 46, members utilizing a Department-issued computer are responsible for the procedures listed in this section.
- B. The only acceptable text for a computer screensaver is "Tallahassee Police Department."

## TALLAHASSEE POLICE DEPARTMENT

---

### Prohibitions –

#### C. Members shall not:

1. Place liquids or food on any part of the computer,
2. Attach adhesive stickers, calendars, photos or similar items to the computer (or for in-car MDCs, to the mount),
3. Attach magnets of any kind to the computer (or for in-car MDCs, to the mount),
4. Add any hardware to the computer without approval of MDC staff,
5. Connect any data storage media which is new or previously utilized in a non-COT computer into a City of Tallahassee computer unless the media has been scanned for viruses using a COT computer, or
6. Exchange computer equipment, parts or peripherals with other members without approval of MDC staff.

### Reporting Computer Operating Problems –

- D. Non-law enforcement related software and application problems (e.g., issues with network passwords and e-mail) should be reported to the COT Technology & Innovations Support Team (aka: Helpdesk).
- E. Law enforcement related software and application problems (e.g., issues with TraCS, LERMS, or PremierOne™ CAD) should be reported to the MDC Unit via the MDC Hotline or e-mail at [tpdmdc@talgov.com](mailto:tpdmdc@talgov.com) (“TPD MDC”).
- F. Computer hardware problems should be reported to MDC Unit via the MDC Hotline or e-mail at [tpdmdc@talgov.com](mailto:tpdmdc@talgov.com) (“TPD MDC”).

### Reporting Other Issues –

- G. For reporting a security breach incident, see subsection XI D 13 – 15 below.
- H. For reporting the loss/theft of a Department-issued computer, see subsection XI D 18 below.

## TALLAHASSEE POLICE DEPARTMENT

---

### V. UTILIZATION OF PERSONALLY OWNED DEVICES FOR CITY BUSINESS

Members are prohibited from transacting Department business by e-mail or text message over a personally owned computer or cellular telephone unless the communication is captured and retained on the COT server.

### VI. E-MAIL PROTOCOLS

A. The COT e-mail system is a resource provided as a business and communication tool for its members and e-mails are considered official Department communications.

B. Members are prohibited from using the COT e-mail system in a manner contrary to established rules of conduct and are specifically prohibited from:

1. Accessing another member's e-mail account without authorization to send, receive or read an e-mail,
2. Sending or forwarding:
  - a. Chain letters,
  - b. Copies of documents in violation of copyright laws, or
  - c. Messages without a legitimate Department business purpose (e.g., political endorsements, commercial activities, requesting donations for non-COT sponsored events).

C. The COT may review, audit, intercept and disclose all matters sent over the e-mail system.

D. Members shall establish and maintain a personalized signature block on the e-mail setup on their Department e-mail account, consistent with the information below.

1. The signature block shall include:
  - a. Member name,
  - b. Member rank and/or assignment,
  - c. "Tallahassee Police Department,"
  - d. Department mailing address (to include city, state, and zip code), and



## **TALLAHASSEE POLICE DEPARTMENT**

---

- e. Contact telephone number(s) (to include area code):
  - 1) Personal telephone numbers are prohibited.
  - 2) If the member is issued a Department cellular telephone, the number shall be provided.
- 2. The signature block shall not include:
  - a. Quotations or sayings, or
  - b. Logos/graphics (Department-related or otherwise).
- E. Members are not authorized to send or forward a Department-wide e-mail without the prior approval of their Bureau Commander or higher Department authority.

### **VII. INTERNET USE**

- A. Access to the Internet via Department-issued computers, cellular telephones and related equipment is a resource provided as a business and communication tool for its members.
- B. When using the COT computer network, to include accessing the Internet and e-mail activity, members are prohibited from the following:
  - 1. Downloading software without authorization from a COT Technology & Innovations (T&I) employee,
  - 2. Disseminating or printing materials, including articles and software, in violation of copyright laws,
  - 3. Sending, receiving, printing, or otherwise disseminating proprietary data, trade secrets, or other confidential information of the COT or Department in violation of policy or written agreements,
  - 4. Operating a business, usurping business opportunities or soliciting money for personal gain,
  - 5. Except when for a legitimate investigative purpose, visiting websites featuring prostitution, sexual activity, pornography, terrorism, espionage or illicit drugs,
  - 6. Gambling or engaging in any other activity in violation of local ordinance, state statute or federal law, or

## **TALLAHASSEE POLICE DEPARTMENT**

---

7. Participating in activities or viewing content which violates any Department written directive or is likely to cause discredit to, or diminish the reputation of, the Department, the COT or the policing profession.

### **VIII. CELLULAR TELEPHONE – ISSUANCE/ACTIVATION PROCEDURES**

- A. Issuance of a cellular telephone is considered a mandatory equipment item for members designated to receive one.
- B. Members receiving a cellular telephone are required to complete the Smartphone Receipt and Acknowledgment form (PD 245) at the time of issuance from the Supply Management Office.
- C. Upon receipt of a cellular telephone, members are responsible for activating the internal software to archive text messages.
  1. The cellular telephone will receive a text from 900080004103, and upon receiving the text, the member shall respond “yes” to complete the archiving activation process.
  2. If the activation text is accidentally deleted, the member is responsible for texting “yes” to 900080004103 to complete the process.

### **IX. CELLULAR TELEPHONE – MEMBER RESPONSIBILITIES**

- A. The protocols of this section augment the CJIS Security Protocols – Member Responsibilities in subsection XI D below.
- B. The utilization of Department-issued cellular telephones is intended for members to:
  1. Facilitate responsive contact and communication between citizens and members (see subsection C below), and
  2. Capture photographs, video recordings and audio recordings as outlined in General Order 19 (Digital Devices and Media).
- C. While on duty, members are responsible for the following:
  1. Providing the phone number to citizens as warranted for anticipated follow-up interaction,
  2. Promptly answering phone calls unless not feasible because of officer safety concerns or interfering with the performance of their duties,

## TALLAHASSEE POLICE DEPARTMENT

---

3. Checking their voicemail once each workday or more often as needed or directed, and
  4. Carrying the phone on their person unless not feasible because of officer safety concerns or inclement weather.
- D. Members shall program and maintain an appropriate personalized voicemail greeting on their Department-issued cellular telephone.
1. The voicemail greeting shall include the member's name and affiliation with the Department (e.g., "This is John Doe of the Tallahassee Police Department"), an invitation for the caller to leave a name, number, and message, and a promise of a return call.
  2. The voicemail greeting may contain other information the member believes is warranted (e.g., work schedule).

### **X. TELECOMMUNICATIONS APPLICATIONS PROTOCOLS**

Members may utilize Department-approved telecommunications applications (see definition) on their Department-issued cellular telephone or Department-issued computer, and the protocols listed below are applicable for such utilization.

- A. Department-approved telecommunications applications are those found available for download in the Department's Mobile Device Manager or installed by a T&I employee.
1. Except as provided in C below, members shall not utilize any written text, messaging or chat features of any telecommunications application except those administered by the COT (which are automatically captured and retained on the COT server).
  2. COT-administered and retained telecommunications applications include Microsoft Teams.
- B. Telecommunications applications shall be utilized only for legitimate Department purposes.
- C. It is recognized the use of Telecommunication Applications is sometimes necessary to facilitate criminal investigations and to capture evidence of crimes. Procedures related to control of criminal evidence may prevent these applications and their evidence from being administered and retained by standard COT systems. Telecommunication applications specifically

## TALLAHASSEE POLICE DEPARTMENT

---

designed for, or used to facilitate, undercover or covert investigations shall be used as follows:

1. Only the Special Investigations Section Commander, the Persons Crimes Section Commander, or higher authority can approve the use of investigative Telecommunications Applications.
  2. Use of investigative Telecommunications Applications is limited to sworn members of the Criminal Investigations and High Risk Offender Bureaus.
  3. All relevant and evidentiary communication generated by or directly received by the member utilizing the investigative Telecommunication Application shall be captured and preserved as evidence per protocols listed in paragraph D below.
    - a. Any other communication (including, but not limited to call logs, messages, pictures, "Snaps", emoticons, etc.) may be captured and preserved in this manner in furtherance of an investigation, to document potential criminal activity, or to ensure the integrity of an investigation.
    - b. Members may consult the Technical Operations Unit for best practices in downloading and preserving evidence from a particular application.
- D. Members shall abide by the operational and evidentiary protocols of Department policies applicable to the utilization of telecommunications applications, including:
1. General Order 42 (Impounding and Controlling of Property and Evidence),
  2. General Order 16 (Digital Audio and Video Recording System),
  3. General Order 18 (Criminal Investigations), and
  4. General Order 19 (Digital Evidence Capturing Devices). (For example, if the telecommunications application is used to facilitate a telephone interview with a person during a criminal investigation, the telephone interview protocols of General Order 18 are still applicable.)
- E. Department members shall not intercept any wire, oral, or electronic communication except pursuant to a lawful investigation and only with proper legal authority derived from applicable state statute or federal code. Such authority may include, but is not limited to:

## TALLAHASSEE POLICE DEPARTMENT

---

1. An Order Authorizing the Interception of Wire, Oral, or Electronic Communications,
  2. An approved Emergency Request to Intercept Wire, Oral, or Electronic Communications, or
  3. Consent.
- F. The direct supervisor (or higher authority within the member's chain-of-command) of any member utilizing a Telecommunication Application shall be aware of all applications being used by the member and shall periodically review the member's use of the application(s) to ensure compliance with Department policy and applicable statutes.

### **XI. CJIS SECURITY PROTOCOLS**

A. This written directive serves to accomplish the Department's responsibilities in regards to:

1. Developing, disseminating and maintaining formal, documented procedures to facilitate the implementation of, and compliance with, the FBI CJIS Security Policy (CSP), and
2. Specifying member rights, privileges and restrictions regarding authorized access to criminal justice information (CJI).

#### **B. Department Responsibilities**

1. The Department is responsible for working cooperatively with T&I employees in managing member access to CJI and in doing so shall adhere to the protocols in Appendix One, Account Management.
2. The Department is responsible for restricting access to digital and physical media containing CJI, and shall ensure:
  - a. Only members who have undergone a fingerprint-based criminal history background check (see section XVII below) and have appropriate security awareness training (see subsection D 1 below) are allowed to handle CJI in any form, and
  - b. Only authorized persons are granted access to media containing CJI.
3. The Department does not allow multiple concurrent active sessions by a member.

## TALLAHASSEE POLICE DEPARTMENT

---

- a. The Department is responsible for establishing access control mechanisms to prevent multiple concurrent active sessions by members.
- b. As described in subsection C 17 below, the COT allows multiple concurrent active sessions for T&I employees.
4. To ensure member access to the COT computer network and CJI is done in a secure manner, the Department utilizes:
  - a. Standard authenticators (user ID and password), and
  - b. For MDC users, advanced authenticators (an RSA device).
5. The Department's access control system and identification protocols provide for the physical protection of CJI and information system hardware, software and media, and include:
  - a. The issuance (and mandatory use) of proximity cards to members and other authorized persons to prevent unauthorized access into the Department building,
  - b. Area access restrictions within the Department building based upon the member's/person's COT job classification to access work areas, hallways, stairwells and elevators to prevent unauthorized access to those areas,
  - c. The requirement of Department building visitors to sign-in at the Duty Office, and
  - d. The requirement of criminal history background checks for vendors who may have unescorted access to the Department building.
6. The Department does not utilize public key infrastructure technology in its encryption processes for CJI.
7. The Department does not utilize Voice over Internet Protocol (VoIP) with any CJI system.
8. The Department does not allow publicly accessible computers (i.e., the CopLogic computer in the Department building lobby) to access CJI.
9. Department-issued computers and cellular telephones meet all CJIS policies and procedures (e.g., NetMotion® as our VPN solution, RSA

## TALLAHASSEE POLICE DEPARTMENT

---

devices for two factor authentication for each MDC, FIPS 140-2 certified encryption).

10. With the sole exception of Rapid ID Devices, the Department prohibits the utilization of Bluetooth technology to access CJI. See General Order 55 (Rapid ID Devices) regarding authorized utilizations of Rapid ID Devices.
11. The Department is responsible for ensuring personally identifiable information (PII) is kept secure.
  - a. PII includes, but is not limited to the following:
    - 1) Social security number,
    - 2) Username and password,
    - 3) Passport number,
    - 4) Credit card numbers and banking information,
    - 5) Biometrics,
    - 6) Data and place of birth,
    - 7) Mother's maiden name,
    - 8) Criminal, medical, financial, educational records, and
    - 9) Photos and video including any of the above.
  - b. Electronic files containing PII must reside within the COT secure computer network.
  - c. Physical files containing PII must reside within locked file cabinets or rooms when not being actively viewed or modified.
12. The Department is responsible for utilizing secure servers for the storage of CJI, and shall ensure:
  - a. The servers are kept in a physically secure area inaccessible to unauthorized persons,
  - b. Access to each server room is limited to persons who are authorized to be present in the room, and

## TALLAHASSEE POLICE DEPARTMENT

---

- c. Access is only granted by utilization of the Department's proximity card system as established in Special Order 10 (Building Security and Evacuation).
13. The Department is responsible for providing designated secure areas for the storage of physical media containing CJI (e.g., offense reports) and ensuring each area is:
- a. Equipped with proximity card swipe reader access, and
  - b. Proximity card access is limited to authorized members.

### C. Technology and Innovation Employees Responsibilities

1. T&I employees are responsible for equipping Department-issued computers, cellular telephones, and related devices with boundary protection tools and spam/spyware to prevent intrusion attacks.
2. T&I employees are responsible for identifying applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws (commonly referred to as patch management).
  - a. T&I employees shall promptly install newly released security patches, service packs, and hot fixes.
    - 1) After receipt from vendors of patch information and updates, T&I employees are responsible for assessing the need to install the information and updates on the COT computer network.
    - 2) If it is determined the information and updates are needed, T&I employees are responsible for testing the updates on network equipment before installing the update to the COT computer network.
    - 3) Once successfully tested, T&I employees are responsible for sending the update to the COT computer network and announcing the update to member/users.
  - b. It is the responsibility of T&I employees to expeditiously address patch issues discovered during security assessments, continuous monitoring or incident responses.
  - c. If a patch is causing network vulnerability, T&I employees are responsible for rolling back the patch/update to lessen the vulnerability.



## TALLAHASSEE POLICE DEPARTMENT

---

- d. T&I employees facilitate automatic updates without member/user intervention.
  - e. Only T&I employees are authorized to conduct patch management.
3. As part of the COT Computer Security Incident Response Team (CSIRT), T&I employees are responsible for adhering to established protocols in response to security alerts and advisories.
- a. T&I employees will monitor and/or receive automated security alerts and advisories as part of their computer security responsibilities and receive alerts and advisories from the following sites on a regular basis:
    - 1) [www.us-cert.gov/ncas/current-activity](http://www.us-cert.gov/ncas/current-activity),
    - 2) <mailto:info@msisac.org>, and
    - 3) <https://technet.microsoft.com/en-us/security>.
  - b. Once an alert has been received or detected (i.e., security thresholds exceeded) and has been determined to be a credible threat, T&I employees will notify the Department and the Local Agency Security Officer (LASO).
  - c. T&I employees and the LASO are responsible for taking the appropriate action(s) depending on the alert (e.g., updating security settings and/or issuing information to all affected members with directions to ensure proper handling of the issue).
  - d. If an alert is determined to be critical or pertinent to COT infrastructure, T&I employees are responsible for promptly notifying appropriate personnel.
  - e. The COT e-mail system will be utilized to make notifications throughout the Department.
  - f. If the COT e-mail system is unavailable, notifications will be made via the established Department chain of command (in person or telephone).
  - g. T&I employees are responsible for recording all alerts and related response actions into a COT alert information log (retained for a minimum of four years).

## TALLAHASSEE POLICE DEPARTMENT

---

4. In the event of a reported security breach incident the LASO is responsible for:
  - a. Determining if the incident resulted in an unauthorized dissemination of CJI,
  - b. If there was an unauthorized dissemination of CJI, ensuring the completion and submittal of an IT Security Incident Response Form and submitting it to the FDLE Information Security Officer (ISO), and
  - c. Making prompt notifications to the CSIRT and directing and/or facilitating their response to the incident.
5. The CSIRT is responsible for the response to a reported security breach incident and a response (full team or partial team) shall be based upon the severity of the incident.
6. The CSIRT will investigate the reported security breach incident to determine if a breach did occur and, if so, determine the level of its impact or threat on the Department. The steps of the investigation include, but are not necessarily limited to, the following:
  - a. Confirming the discovery of a compromised resource,
  - b. Evaluating the circumstances of the reported security breach incident,
  - c. Identifying the system(s) of information affected,
  - d. Reviewing all preliminary details of the incident,
  - e. Classifying the impact on the Department (see subsection 7 below),
  - f. Determining where and how the security breach occurred (i.e., identifying the source of compromise and involved timeframe, reviewing the COT computer network to identify all compromised or affected systems),
  - g. Examining appropriate system and audit logs for further irregularities, and documenting all internet protocol (IP) addresses, operating systems, domain system names and other pertinent system information,
  - h. Initiating measures to contain and control the security breach to prevent further unauthorized access, and

## TALLAHASSEE POLICE DEPARTMENT

---

- i. Documenting the response actions throughout the process from initial detection to final resolution.
7. Based upon the criteria in COT 405 (Computer Security Incident Response), the CSIRT shall classify a security breach incident into one of three categories based on the severity of incident – Class 1, Class 2, Class 3:
  - a. **Class 1 incidents** –
    - 1) Localized, minor and may not require full CSIRT involvement.
    - 2) This type of incident will be reviewed by appropriate T&I employees as determined by the LASO.
    - 3) The CSIRT may escalate a Class 1 incident into a Class 2 incident if deemed appropriate.
    - 4) Examples of a Class 1 incident include localized virus attacks and missing or stolen devices or equipment which contain CJI.
  - b. **Class 2 incidents** –
    - 1) Localized, high-impact situations which require full CSIRT involvement.
    - 2) The LASO will determine the need to escalate to a Class 3 incident and if there is a need for assistance from other agencies.
    - 3) Examples of a Class 2 incident include coordinated and/or distributed virus attacks, any action causing a denial of service to internal systems or external non-COT systems and compromise of customer data.
  - c. **Class 3 incidents** –
    - 1) Class 3 incidents are similar to Class 2 incidents but have a system-wide impact.
    - 2) The LASO is responsible for promptly reporting a Class 3 incident to the City Manager via the chain of command.
8. T&I employees are responsible for authorizing, monitoring and controlling all methods of remote access to the COT network.

## TALLAHASSEE POLICE DEPARTMENT

---

- a. The rationale for allowing remote access includes the following:
    - 1) Third party vendors who have sold the COT hardware, software, or communications systems who need access to upgrade or repair those systems, and
    - 2) Members who may need access from remote locations (e.g., residences, hotel rooms) for a work-related purpose.
  - b. Remote access requires prior approval, as follows:
    - 1) For members: Their immediate supervisor and the LASO (see subsection D 16 below for approval criteria).
    - 2) For vendors: The LASO is the sole approval authority for vendors (see subsection c below for approval criteria).
  - c. For a third party vendor to be approved for remote access, the following requirements shall be met:
    - 1) The vendor representative must sign the *CJIS Security Agreement* and the *COT Third Party Access Agreement*, and
    - 2) Each person representing the vendor in the work to be completed must:
      - a) Successfully complete the CJIS online security training,
      - b) Submit to being fingerprinted, and
      - c) Successfully pass a criminal history background check.
  - d. The technical process for enabling remote access involves the following:
    - 1) For members, the installation of NetMotion Mobility® on the device to be used for remote access.
    - 2) For third party vendors, ensuring the installation of NetMotion Mobility® and/or other encryption deemed warranted by the COT on all devices to be used for remote access.
9. T&I employees are responsible for ensuring the COT servers containing CJI are encrypted with FIPS 140-2 certified encryption.

## TALLAHASSEE POLICE DEPARTMENT

---

10. T&I employees are responsible for protecting CJI from accidental or intentional unauthorized disclosure, alteration, destruction or misuse throughout its life cycle, to include:
  - a. Ensuring CJI (digital or physical) is securely handled, transported and stored to prevent unauthorized access,
  - b. Prohibiting unauthorized persons from accessing or viewing CJI, and
  - c. Protecting and controlling documents or media containing CJI during transport outside of controlled areas to prevent it being accessible or visible to unauthorized persons, to include:
    - 1) Physically securing any such document or media in a sealed envelope or container,
    - 2) Avoid becoming involved in non-essential tasks/actions unrelated to the transport and delivery of the CJI, and
    - 3) Prohibiting an unauthorized person from transporting CJI.
11. T&I employees are responsible for working cooperatively with the Department in managing member access to CJI and in doing so shall adhere to the protocols in Appendix One, Account Management.
12. For members with an MDC, T&I employees are responsible for establishing the member's user access via the RSA device and issuance of the RSA device to the member.
13. In the event of a reported lost or stolen RSA device, T&I employees are responsible for disabling the device and reissuing a replacement to the affected member.
14. T&I employees are responsible for establishing and maintaining a Wi-Fi log for all COT-managed wireless access points and reviewing the logs at least monthly.
15. In the event of a reported loss or theft of a Department-issued computer, cellular telephone or RSA device, the LASO is responsible for promptly notifying the FDLE ISO of the loss/theft (via the IT Security Incident Response Form).
16. T&I employees have responsibilities in the disposal of certain physical media containing CJI and PII (see section XIII below).

## TALLAHASSEE POLICE DEPARTMENT

---

17. The COT allows multiple concurrent active sessions for T&I employees engaged in troubleshooting and other work-related activities.
18. On a weekly basis, T&I employees shall review audit logs for CJI systems.
  - a. The review shall include logins, password attempts and other actions for privileged accounts.
  - b. The audit logs shall be maintained for at least one (1) year.

### D. Member Responsibilities

1. Accessing or viewing CJI on Department-issued computers, cellular telephones, related equipment or via the COT computer network is limited to designated members who have successfully completed required training (e.g., CJIS online security training, limited or full access training, DAVID certification, ELVIS training).
2. It is the responsibility of all members to protect CJI and PII from accidental or intentional unauthorized disclosure, alteration, destruction or misuse throughout its life cycle.
  - a. Members are responsible for ensuring CJI/PII (digital or physical) is securely handled, transported and stored to prevent unauthorized access.
  - b. Members are prohibited from allowing unauthorized persons to access or view CJI/PII.
  - c. Members shall only access, view, and/or use CJI/PII for the administration of criminal justice or an authorized noncriminal justice purpose (e.g., employment background check).
  - d. Members shall abide by all applicable FCIC/NCIC, CJIS, DAVID, ELVIS and MMUR rules, regulations and operating procedures.
  - e. Members shall properly dispose of CJI/PII as described in section XIII below.
3. In addition to the protocols of subsection 2 above, members are responsible for adhering to the protocols listed below.

## TALLAHASSEE POLICE DEPARTMENT

---

- a. Locking their Department-issued computer (in a manner requiring User ID and password for access) when away from their computer work area.
- b. Not leaving their Department-issued MDC or cellular telephone unattended in an unsecure area at any time.
- c. Not utilizing another member's active network session for accessing public safety information or CJI/PII.
- d. Not allowing a non-member to have access to the COT computer network or utilize any Department-issued computer, cellular telephone, or related equipment unless the equipment is designed for such use (e.g., CopLogic™ computer in the Department building lobby).
- e. Not leaving documents or media containing CJI/PII in an unsecured area or in an area accessible or visible to unauthorized persons (e.g., on the dashboard of a vehicle).
- f. Ensuring physical media containing CJI/PII (e.g., offense report, traffic crash report) is stored in designated secure areas designed for authorized member access only (e.g., Records Unit), and ensuring:
  - 1) All physical media containing CJI/PII is stored in a locked filing cabinet or desk within the designated secure area and only removed when needed for operational purposes, and
  - 2) Any removal and return of physical media containing CJI/PII is documented on the appropriate log.
- g. Protecting and controlling documents or media containing CJI/PII during transport outside of controlled areas to prevent it being accessible or visible to unauthorized persons, to include:
  - 1) Physically securing any such document or media in a sealed envelope or container,
  - 2) Avoid becoming involved in non-essential tasks/actions unrelated to the transport and delivery of the CJI/PII,
  - 3) Prohibiting an unauthorized person to transport CJI/PII, and
  - 4) For CJI, documenting the transfer of information on a secondary dissemination log as described in subsections XII D and E below.

## TALLAHASSEE POLICE DEPARTMENT

---

4. In addition to the protocols of subsections 2 and 3 above, members shall adhere to the procedures listed below concerning computer system User ID and passwords.
  - a. Members may change their password at any time.
  - b. Members shall change their password when:
    - 1) Directed to do so by the COT (computer-prompted or otherwise), or
    - 2) The password is suspected or known to have been disclosed to another person.
  - c. When establishing a password, members shall ensure it follows these mandated attributes:
    - 1) Be a minimum length of 20 characters,
    - 2) Contain at least one (1) number and one (1) special character (e.g., @, #),
    - 3) Not be a dictionary word or proper name,
    - 4) Not be the same as their User ID, and
    - 5) Not be identical to the previous 10 passwords.
  - d. Members shall not:
    - 1) Allow the password to be displayed when entered,
    - 2) Divulge their User ID or password to another person,
    - 3) Display or transmit their password in an unsecure manner,
    - 4) Use another member's User ID or password to access the COT computer network, public safety information or CJI/PII, or
    - 5) Cache their User ID or password for access to the systems or applications used to process or store CJI/PII.
5. In addition to the protocols of subsections 2 – 4 above, members with an RSA device are responsible for the following:



## TALLAHASSEE POLICE DEPARTMENT

---

- a. While on duty or working secondary employment, maintaining possession of their RSA device at all times,
  - b. When off duty, securely storing their RSA device out of sight from other persons,
  - c. Not allowing other persons to utilize their RSA device,
  - d. Renewing their RSA device with the MDC Unit when expired, and
  - e. Promptly reporting to their chain of command, the Supply Management Office and the MDC Unit if their RSA device:
    - 1) Has been lost or stolen, or
    - 2) Appears to be compromised or malfunctioning.
6. Members are responsible for ensuring their FCIC/CJIS-related certification is up-to-date.
7. Members are only authorized to access and utilize Emergency Contact Information (ECI) associated with a driver or vehicle record in DAVID or ELVIS in the event of a true emergency (e.g., missing person, natural disaster, or traffic crash where there is serious bodily injury or death and next of kin notification needs to be made).
- a. ECI shall not be accessed or utilized for investigative purposes (i.e., identifying and/or locating suspects) without the consent of the person to whom such ECI applies.
  - b. A member accessing and/or utilizing ECI shall document the access/utilization (and the reason for it) in the appropriate Department report.
8. Access to physically secure locations will be limited to members authorized to access or view CJI/PII or perform other authorized duties.
9. Members shall ensure physically secure locations are properly locked when unattended.
10. When a member's Department-issued computer or cellular telephone is displaying CJI or PII, the member is responsible for positioning the computer/telephone in such a way to prevent unauthorized persons from accessing or viewing the information.

## TALLAHASSEE POLICE DEPARTMENT

---

11. Members are authorized to access FCIC/NCIC, CJIS, TraCS, DAVID, ELVIS and MMUR only on Department-issued computers and cellular telephones, and are prohibited from accessing, processing, storing, or transmitting CJI on any personally-owned equipment.
12. Members should not disseminate CJI obtained directly from FCIC/NCIC via e-mail.
13. In the event a member receives information regarding security alerts or advisories from an entity other than T&I, the member is responsible for promptly forwarding the information to T&I.
14. Members shall promptly report to the LASO any security breach incident (see definition).
15. Members reporting a security breach incident may do so by either:
  - a. In person contact with the LASO during normal business hours, or
  - b. By accessing the FDLE IT Security Incident Response Form on the TPD-Net Forms File, completing the form and submitting it to the LASO via e-mail at [tpdlaso@talgov.com](mailto:tpdlaso@talgov.com).
16. If a security breach incident occurs on a member's mobile device (i.e., smartphone, MDC) the member shall leave the device on and report the incident as described in subsection 14 above.
17. A member's remote access to the COT computer network (e.g., accessing the network from home) requires the approval of their immediate supervisor and the LASO.
  - a. Remote access will be approved only for work-related needs.
  - b. Remote access will be approved only for devices containing NetMotion Mobility®.
  - c. The security protocols of this written directive and the CSP are equally applicable to remote access situations.
  - d. A member's remote access may be revoked at any time for cause (e.g., unsatisfactory work performance, non-compliance with security protocols).
18. Members are responsible for safeguarding PII, and shall:

## TALLAHASSEE POLICE DEPARTMENT

---

- a. Only access, view or utilize PII for a legitimate Department business purpose (e.g., criminal investigation, employment background check),
  - b. Only access PII on a Department-issued computer or Department-issued cellular telephone,
  - c. Not access, process, store, or transmit PII on any personally-owned equipment,
  - d. Not download PII to a desktop computer or mobile device (e.g., MDC, mobile phone),
  - e. Not create duplicate copies of PII, and
  - f. Not transport PII to a non-secure location (e.g., personal residence).
19. In the event a member loses or has their Department-issued computer or cellular telephone stolen, the member is responsible for the protocols listed below.
- a. The member shall make prompt notification of the loss/theft to the LASO.
    - 1) During normal business hours, the notification may be made in person, by telephone or e-mail ([tpdlaso@talgov.com](mailto:tpdlaso@talgov.com)).
    - 2) During non-business hours, the notification shall be made via e-mail.
  - b. The member shall ensure their chain of command (up to and including the Bureau Commander) and the MDC Unit are made aware of the loss/theft and notification to the LASO.
  - c. The CSP requires the LASO to notify the FDLE ISO of any loss or theft of a cellular telephone or similar digital device which contains CJI or PII.
  - d. Notification to FDLE shall be made by the completion and submission of the IT Security Incident Response Form.

### E. FCIC Agency Coordinator (FAC) Responsibilities

1. The FAC shall identify the Department's physically secure locations where CJI will be accessed, processed and/or stored.

## TALLAHASSEE POLICE DEPARTMENT

---

2. The FAC is responsible for working cooperatively with the LASO in deactivating a member's access to CJIS, DAVID, and ELVIS information upon separation from COT employment or termination of duties requiring such access. See Appendix One (Account Management) for more information on deactivation processes.
3. The FAC is the repository of member FCIC/CJIS-related and DAVID certification and recertification records, and ELVIS training records.
4. In compliance with the CSP, the FAC is responsible for making notifications to the appropriate agency (e.g., FBI, FDLE, DHSMV) in situations affecting, or potentially affecting, the security of CJI. Such situations include, but are not limited to, the following:
  - a. Discovered misuse of CJI,
  - b. An authorized member has been arrested for a felony, or
  - c. There has been a compromise of a Department system utilized to access CJI.

### **XII. RETENTION AND DISSEMINATION PROTOCOLS**

- A. Retention of public safety information is governed by the records retention schedule for law enforcement published by the Florida Department of State (GS-2).
- B. Any release of CJI must comply with all applicable statutes (e.g., FS Chapter 119) and regulations (e.g., FCIC/NCIC, CJIS, DAVID, ELVIS).
- C. Members are authorized to disseminate CJI, to include CJI which contains PII, only to other authorized members or other criminal justice agencies and only for the administration of criminal justice or an authorized noncriminal justice purpose (e.g., employment background check).
  1. Before any dissemination of CJI, the member providing the CJI shall validate the requestor is an authorized recipient.
  2. Authorized recipients include only:
    - a. Members who are engaged in the administration of criminal justice or an authorized noncriminal justice purpose (e.g., employment background check), and

## TALLAHASSEE POLICE DEPARTMENT

---

- b. Employees of other criminal justice agencies who are engaged in the administration of criminal justice or an authorized noncriminal justice purpose (e.g., employment background check).
    3. The validation of the requestor of CJI includes:
      - a. The member's personal knowledge of the requestor as an employee of a criminal justice agency, or
      - b. Verification the requestor is an employee of a criminal justice agency by straightforward and reasonable means (e.g., speaking with other members who know the requestor, querying professional website information and other sources for confirmation of requestor credentials).
  - D. In the event a member provides CJI to an authorized person who is not a member, the distribution of the information shall be documented and maintained on a secondary dissemination log:
    1. Individual work units are responsible for maintaining their own secondary dissemination logs.
    2. Secondary dissemination logs shall reflect, at a minimum:
      - a. Date of release,
      - b. To whom the information relates,
      - c. To whom the information was released (to include person's full name, their badge or identification number, and agency name),
      - d. The State Identification (SID) and/or the FBI number(s),
      - e. The purpose code, and
      - f. The reason for which the information was released.
  - E. The Department has information sharing agreements with local and state criminal justice agencies, but the existence of such an agreement does not negate the mandate to document the distribution of CJI on a secondary dissemination log or other Department-approved audit logs.

### **XIII. MEDIA DISPOSAL PROTOCOLS**

## TALLAHASSEE POLICE DEPARTMENT

---

- A. The protocols in this section are applicable when digital or physical media contains CJI and PII, and members and T&I employees have responsibilities in this section.
- B. Digital Media (any type of electronic storage media to include computer hard drives, cellular telephones, and removable/transportable media such as flash drives, external hard drives, or digital memory cards):
1. For computer hard drives, cellular telephones, and external hard drives, T&I employees are responsible for degaussing and physically destroying the equipment.
  2. The T&I employee responsible for the digital media disposal outlined above is responsible for ensuring a sworn member is present for the destruction of the equipment.
  3. Sworn members shall cooperate with T&I employees in the destruction of digital media.
  4. For flash drives and digital memory cards, members are responsible for sanitizing (i.e., overwriting three times or degaussing) the equipment prior to it being:
    - a. Physically destroyed (e.g., cut up or shredded), or
    - b. Released for reuse by a person not authorized to view CJI or PII.
  5. Members are responsible for ensuring inoperable digital media is physically destroyed (e.g., cut up or shredded).
  6. The Department is responsible for ensuring the sanitization or destruction process for digital media is documented in a manner consistent with the CSP.
  7. When disposing of digital media, members shall ensure the following:
    - a. The sanitizing or shredding process does not allow an unauthorized person to view CJI or PII, and
    - b. If the sanitizing or shredding process is carried out by an unauthorized person, an authorized member witnesses the sanitizing or shredding process.
- C. Physical Media (Printed documents or imagery):

## TALLAHASSEE POLICE DEPARTMENT

---

1. Physical media shall be securely disposed of when no longer required for a legitimate Department business purpose.
2. When disposing of physical media, members and T&I employees shall ensure the following:
  - a. The disposal is by shredding,
  - b. The shredding process does not allow an unauthorized person to view CJI or PII,
  - c. If the shredding process is carried out by an unauthorized person, an authorized member witnesses the shredding process, and
  - d. For *original* records, adhering to the destruction of records protocols in General Order 17 (Records Management).

### **XIV. CJIS VALIDATIONS**

- A. Designated members of the Records Unit are responsible for validating records entered into CJIS for accuracy and retention.
- B. Members who are authorized to conduct CJIS validations are responsible for conducting such verifications in a timely manner in order to ensure system accuracy and effectiveness.

### **XV. AUDITS AND INSPECTIONS**

- A. In order to ensure compliance with COT and Department policy, authorized COT employees and Department supervisors and other authorized members may at any time and without notice inspect:
  1. Any and all files, messages and data stored in all areas of the COT computer network assigned to the Department, and
  2. Any and all Department-issued computers, cellular telephones and related devices.
- B. Oversight and inspection activities include, but are not necessarily limited to, the following:
  1. COT and Department internal audits,
  2. Monitoring Internet and e-mail use,

## **TALLAHASSEE POLICE DEPARTMENT**

---

3. Criminal investigations and administrative investigations (i.e., internal investigations, special investigations, contact reports).
- C. FDLE is authorized to conduct scheduled and unscheduled CJIS compliance and technical security audits.
- D. DHSMV is authorized to conduct scheduled and unscheduled compliance audits.
- E. Supervisors are authorized to inspect members' computer workstations (office or vehicle) at regular and frequent intervals, with or without prior notice, to ensure policy compliance.
- F. Members are required to cooperate with all audits and inspections of their Department-issued computer, cellular telephone, and data utilization.

### **XVI. VIOLATIONS AND SANCTIONS: FCIC/NCIC/CJIS/DAVID/ELVIS/MMUR**

- A. The Department will investigate allegations of member misuse of FCIC/NCIC, CJIS, DAVID, ELVIS or MMUR.
- B. The Chief of Police is authorized to suspend a member's access to FCIC/NCIC, CJIS, DAVID, ELVIS or MMUR during an investigation of misuse of such systems.
- C. Misuse of FCIC/NCIC, CJIS, DAVID, ELVIS or MMUR can subject a member to:
  1. Discontinuation of access to those systems,
  2. Progressive discipline up to and including termination of COT employment,
  3. Civil sanctions/fines, and
  4. Criminal charges.
- D. The FBI, FDLE, DHSMV, and the Florida Department of Health reserve the right to deny access to their respective systems to any member who has a sustained case of misuse of FCIC/NCIC, CJIS, DAVID, ELVIS or MMUR information.

### **XVII. BACKGROUND CHECKS – MEMBERS AND NON-MEMBERS**



## TALLAHASSEE POLICE DEPARTMENT

---

- A. The Department will conduct state and national fingerprint-based criminal history background checks and other criminal history background checks on the following persons:
  - 1. Members who are authorized to access CJI as part of their work assignment,
  - 2. Members and non-members who may have unescorted physical or remote access to a physically secure location, and
  - 3. T&I employees who maintain/support information technologies used to process, transmit or store CJI.
- B. If the records checks reveal no arrests, access to CJI may be granted.
- C. If the records checks reveal an arrest record of any kind:
  - 1. The Department will consult the FDLE Guidelines for CJIS Access and notify FDLE for a review of the case, and
  - 2. The FDLE is responsible for notifying the Department in writing of their decision regarding access.

### **XVIII. CRIMEVIEW PROTOCOLS**

- A. CrimeView is a Department-authorized software program which queries specific data available in the CAD and RMS to determine location/time based information to assist officers in policing their assigned areas of responsibility.
- B. Although officers are authorized to view and utilize the information from CrimeView, the only members authorized to print CrimeView information are Crime Intelligence Analysts of the Crime Analysis Unit (CAU).
- C. The CAU is the only Department work unit authorized to disseminate CrimeView information to non-Department entities or persons.
- D. Inclusion of CrimeView information in offense reports shall be limited to those situations as outlined in CrimeView utilization training.

History: *previous title (computer and data utilization)* - issued 06/18/2014, revised 12/30/2014, 01/18/2016, 12/27/2016, 06/19/2018 (title change – *computer, cellular telephone and data utilization*), 05/22/2019, 12/10/2019, and 05/01/2020.

TALLAHASSEE POLICE DEPARTMENT

---

**GENERAL ORDER 77 – COMPUTER, CELLULAR TELEPHONE  
AND DATA UTILIZATION**

**APPENDIX ONE**

**ACCOUNT MANAGEMENT**

This appendix contains the established protocols for the administration and management of user accounts for authorized members (“users”) in accessing criminal justice information (CJI) in compliance with the CSP.

**I. LOCAL AGENCY SECURITY OFFICER (LASO)**

- A. The LASO is the point of contact for all user accounts.
- B. The LASO is responsible for ensuring the proper management of information system accounts to include establishing, activating, modifying, reviewing, disabling and removing user accounts on all CJI systems, and shall:
  - 1. Establish, activate and grant member access based upon:
    - a. Valid need-to-know and need-to-share criteria determined by the member’s COT job classification (e.g., police officer), and
    - b. The member’s satisfaction of any required security criteria (e.g., CJIS on-line certification),
  - 2. Ensure designated members successfully complete the requisite training to maintain their FCIC/CJIS-related and DAVID certifications,
  - 3. Establish a complete and up-to-date list of members with authorized access to CJI,
  - 4. Review and modify member access as warranted (e.g., work assignment change),
  - 5. Disable and/or remove member access as warranted (e.g., separation from COT employment), and
  - 6. At least annually, conduct a documented validation of members who have authorized access to CJI.

**II. ACCOUNT CREATION**

- A. Upon completion of appropriate state and national fingerprint-based criminal history background checks, the Department will notify the LASO and provide the following information regarding the member/user:
  - 1. Full name,
  - 2. Date of birth,
  - 3. Social security number,
  - 4. Start date of COT employment,
  - 5. If applicable, the identification information for the Department-issued MDC, and
  - 6. System(s) access and permissions of the member.
  
- B. The LASO is responsible for ensuring the creation and establishment of a Windows Domain account for the member/user.
  - 1. Each account is uniquely identified by a user name derived from the member/user's last name followed by the first three letters of the member/user's first name.
  - 2. All accounts are created to ensure a unique username for every member/user.
  - 3. Each domain account is assigned a temporary password and will be set up to require the member/user to create a new password upon activating the first session.
  - 4. The password for the account must adhere to COT password requirements.
  
- C. The LASO is responsible for ensuring the establishment of an account for the SmartCop RMS and CAD system for the member/user utilizing the same username requirements.
  
- D. The LASO or designee will identify the level of authority for the member/user (e.g., sworn member, records technician) for each application.
  
- E. The LASO is responsible for ensuring the initial credentials and temporary password are provided to each member/user's supervisor.

## TALLAHASSEE POLICE DEPARTMENT

---

- F. Only after the completion of the requisite paperwork and background checks may a member/user be issued Department equipment for their COT job classification. Such equipment includes, but is not necessarily limited to:
  - 1. Proximity card, and
  - 2. Computer (and, if applicable, an RSA device).
- G. Subsequent changes to any issued equipment cited in subsection F above shall be completed only with supervisory approval and documented via the appropriate equipment receipt.
- H. The LASO is responsible for ensuring each member/user has been granted proper access to each information system needed for the member's COT job classification.

### III. ACCOUNT MODIFICATION

In the event of a member's change of employment status (e.g., promotion, demotion, suspension, leave of absence, separation of COT employment) the Department (i.e., member's immediate supervisor, Employee Resources Director, Bureau Commander) is responsible for notifying the LASO of the change of status to ensure appropriate access changes are made to systems and applications.

- A. For a promotion or demotion –
  - 1. The Department is responsible for promptly notifying the LASO of the promotion or demotion, and
  - 2. The LASO is responsible for ensuring:
    - a. All affected systems and applications are updated to reflect the current status of employment, and
    - b. The changes are documented in the active directory.
- B. For a suspension or leave of absence –
  - 1. The Department is responsible for promptly notifying the LASO of the temporary change to the member/user's account.
  - 2. The LASO is responsible for ensuring temporary deactivation of the member/user's account on each system and application.

## TALLAHASSEE POLICE DEPARTMENT

---

3. The Department is responsible for collecting the member's proximity card and, if applicable, their MDC and RSA device.
  4. The affected member/user is responsible for relinquishing the items cited in subsection 3 above to their supervisor (or other proper Department authority) upon direction to do so.
  5. Upon member/user reinstatement:
    - a. The LASO is responsible for ensuring the reactivation of the member/user's accounts on all affected systems and applications,
    - b. The Department will return Department-issued equipment to the member/user following established protocols, and
    - c. The member/user is responsible for ensuring the affected accounts are active.
- C. For separation of COT employment –
1. The Department is responsible for promptly notifying the LASO of the member/user's separation of employment,
  2. The LASO is responsible for ensuring the disabling of all member/user accounts on each system and application for the former member is completed no more than seven (7) working days from the date of notice, to include:
    - a. Disabling of the e-mail account, and
    - b. The removal of:
      - 1) All access controls,
      - 2) Any remote access ability, and
      - 3) All COT computer system permissions.
  3. The LASO is responsible for ensuring the former member/user account information is placed in the Disabled User Organizational Unit within the active directory.

**IV. ACCOUNT VALIDATION**

- A. The LASO is responsible for ensuring a quarterly validation of Department user accounts and access privilege levels occurs.
- B. The LASO is responsible for ensuring the date and time of the validation are documented on the Agency Validation Form.
- C. The LASO is responsible for ensuring the verification of all active accounts being current and up-to-date.
- D. The LASO is responsible for ensuring any changes made contemporaneous to the quarterly validation are documented.