VIA Transit Police Department

Standard Operating Procedures

Section 406 CJIS Security

Office with Primary Responsibility:	COP	Effective Date: Prior Revision Date:	March 1, 2022 November 21, 2020
Office(s) with Secondary Responsibilities:	TAC	Number of Pages:	7
Forms Referenced in Procedure:	TLETS Security Incident Response Form	Related Procedures:	ALL

.01 *TLETS Terminal, Mobile Data Terminal and CJIS Security*

A. Purpose: To establish guidelines for use and security of the department-issued TLETS Terminal, Mobile Data Terminal (MDT) equipment and related CJIS information. Failure to comply with this policy can result in disciplinary action or termination.

B. Policy: It shall be the policy of VIA Metropolitan Transit Police Department to protect the integrity of the CJIS database and all data and information obtained through use of Mobile Data Terminals and/or hard-wired TLETS terminals by strictly following the procedures outlined in this General Order.

C. Definitions:

1. TLETS Terminal – This term includes all computers (normally desktop) that have access, via wireless or hardwired network, to TLETS, TCIC, NCIC or any law enforcement database.

2. MDT -Mobile Data Terminal. This term includes all computers that have access, via wireless or hardwired network, to TLETS, TCIC, NCIC or any law enforcement database.

3. Secure location -This term includes the areas of VIA Metropolitan Transit Police Department that are not open to the public and accessible only by authorized personnel. This term also includes official police vehicles that are locked and/or attended by authorized sworn police personnel.

4. Non-secure location -This term includes all locations not defined as "secure location" above.

D. Procedures:

1. CJIS, TLETS, TCIC and NCIC data shall be accessed ONLY from secure locations, as defined above.

2. Each person authorized to access Terminal/MDT data shall receive security awareness training within six months of appointment or employment and thereafter at least every two years, in accordance with CJIS policy; this training will be documented.

3. Maintain a roster and/or agency-issued credentials (officer badge, access card, etc.) of authorized personnel with unescorted access into physically secure areas.

4. When transporting non-law enforcement personnel in police vehicles, officers will close the screen of the MDT or position it in a manner that will prevent unauthorized viewing of MDT data. TLETS terminal screens shall be positioned to prevent unauthorized viewing.

5. User/Operator List shall be reviewed annually and as needed; document when this was performed. Changes in authorized personnel (creating, activating, modifying, disabling & removing accounts) will be immediately reported to TCIC Training section.

6. All printouts of CJIS data shall be promptly filed with the corresponding incident records. Otherwise, such printouts should be promptly shredded; if not shredded, then incinerated. Disposal or destruction is witnessed or carried out by authorized personnel.

7. All storage media containing or used for CJIS data that is no longer used shall be secure-formatted using methodology that over-writes all data in three iterations or degaussed prior to disposal or release for reuse by unauthorized personnel; if no longer needed, media will be destroyed. Inoperable electronic media shall be physically destroyed. Sanitation or destruction is witnessed or carried out by authorized personnel.

8. The Department shall keep a list of all MDT IDs and contact(s) so that devices can be promptly disabled, should the need arise.

9. The local CJIS network equipment shall be located in a physically secure location.

10. All law enforcement vehicles containing MDTs shall be securely locked when not in use.

11. All computers used for processing CJIS data shall have anti-virus software installed; all will have latest available updates for the operating system & anti-virus. MDT(s) shall have a personal firewall enabled

12. Employ a Formal Incident Response Plan. It shall be the responsibility of each authorized user to report any violations of this security policy up the chain-of-command and/or proper authorities.

13. No personal hardware (PC, laptop, etc.) or software shall be allowed on the agency's TLETS network.

14. No publicly accessible computers shall be allowed on the agency's TLETS network.

15. The agency shall authorize and control information system-related items entering and exiting the physically secure location.

16. The agency shall establish a Security Alert and Advisories process.

B. Best Practices:

1. Periodically check to ensure Servers/Terminals/MDTs connected to the CJIS network are receiving the latest updates in regards to the Operating System & Antivirus software; ensure personal firewalls are enabled on MDTs; ensure Sessions are locked within thirty (30) minutes on non-dispatch Terminals. Take appropriate action if required.

2. Periodically check physically secure location(s) to ensure safeguards such as locks are in working order; Doors are closed & properly secured; Terminals are not viewable by unauthorized personnel. Take appropriate action if required.

3. Periodically check to ensure that all network components (routers, firewalls, switches) that process CJIS information are still supported by the manufacturer. If warranties/contracts are in place, ensure they are valid and not out of date. Take appropriate action if required.

4. Periodically check pertinent documents to ensure they are up to date. Take appropriate action such as making editing changes or replacement if required.

.02 Procedures for Secure Disposal of Electronic and Physical Media

A. Electronic Media Sanitization and Disposal: The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic 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.

B. 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.

C. Definitions

Destruction - destruction includes, but is not limited to:

1. Shredding
2. drilling holes into hard drives
3. degaussing with strong magnets
4. physically breaking into pieces
5. incineration
6. etc.

Media - Media includes, but is not limited to:

1. Paper
2. hard drives
3. CDs
4. DVDs
5. Tape
6. USB “thumb drives”
7. etc.

D. Procedure All data drives from the agency computers, laptops, servers, networked printers / copiers, tablets, smartphones that will be redeployed to other departments, sold, or disposed of will need to be wiped before reimaging or disposal. Wiping the drives will be accomplished by booting the devices and using a commercially available boot and wipe software method first. The Technical Support Lead will log each system’s drive information into a log, recording date/time of wipe and which system the drive was removed from as well which system the drive went into. If sold or disposed of, the information will indicate this information, including company sold to, or method of disposal. This process will be witnesses or carried out by authorized staff. All paper media, DVDs, USB drives, tapes are first cross cut shredded, if possible, then incinerated when no longer needed.

.04 *Incident Handling and Response Plan*

A. TLETS Security Incident Response Plan: There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile. The following establishes an operational incident handling procedure for VIA Metropolitan Transit Police Department CJIS, TCIC/NCIC, and TLETS information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; track, document, and report incidents to appropriate Agency’s Name personnel, TCIC agency officials and/or authorities. TAC Officer Stephen Baker is the department’s point-of-contact for security-related issues and will ensure the incident response reporting procedures are initiated at the local level. As the criminal justice community becomes more dependent on global network technology, the reasons for the attacks can be accidental or malicious. The effects of these intrusions can range from embarrassment, to causing the inability to function, to the loss of human life. Because incidents can have many possible consequences that range from slight to catastrophic, priorities must be considered when evaluating and processing incidents. The following five priorities should be evaluated when an incident occurs:

1. Priority 1 - Protect human life and people's safety.
2. Priority 2 - Protect classified data.
3. Priority 3 - Protect Sensitive but Unclassified data.
4. Priority 4 - Prevent damage to systems (e.g., loss/alteration of software and files, damage to drives, etc.).
5. Priority 5 - Minimize disruption of computing resources.

B. **Reporting Information Security Events:** The department will promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems 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 department will use email to expedite the reporting of security incidents. All Dispatchers will 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 information security events and weaknesses as quickly as possible to the Support Services Supervisor.

C. **Reporting Procedures for Suspected and Actual Security Breaches:** If you become aware of any policy violation or suspect that your password may have been used by someone else, first, change your password and, then, report the violation immediately to the Support Services Supervisor.

D. **Reporting Information on Mobile Devices** Mobile devices present unique security challenges from suspected loss of device control, device lost or stolen (including outside U.S.) or device becomes compromised. Both the device type and connectivity methods installed and configured on the device will impact the overall risk scenario associated with the device. Each device type and policy defined is based on the inherent risk associated to such device.

1. Laptop devices: The laptop device type 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 traditional laptop computers and '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.

2. Tablet devices: The tablet device type 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) and have limited operating feature sets. Operating systems designed specifically for the mobile environment where battery life and power efficiency are primary design drivers.

3. Pocket devices/Handheld devices: The pocket/handheld device type 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. 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. This includes rooting, jail breaking 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 intentional actions or accidental user actions). Knowing the device lock state, duration of loss, total loss of CJI stored can help determine any capabilities for remote wiping or device tracking. 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.

E. **Reporting Procedures for Mobile Devices:** Personnel shall report immediately any incident involving loss of device control, device lost or stolen (including outside U.S.) or device becoming compromised to your supervisor, TAC, or agency management so steps can be taken to resolve the situation and/or mitigate the risk. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the department will use email to expedite the reporting of security incidents.

F. **Virus Reporting Procedures and Collection of Security Incident Information**

1. Upon identifying problem, if applicable, disconnect the TLETS coax cable from the TLETS Hughes modem.

2. Notify TAC Officer Stephen Baker and the appropriate Chain-of-Command.

3. Notify Raul Botan - Information Technology Security Administrator at 210-362-2345 and LASO Lt. George Aguilar.

4. Notify the TLETS Operations Intelligence Center (OIC) at 1-888-DPS-OIC0 (1-888-377-6420)

5. Identify who will run agency traffic in the meantime while the problem is being resolved.

6. Notify Contractor(s) of situation, if required.

7. Compile information for completing an Information Security Response Form

8. Suspected cause for incident (Name, virus, etc.)

9. Was Antivirus software running at the time of infection?

10. When and how was the problem first identified?

11. Has local IT staff been notified and are implementing a resolution?

12. Number of workstations, laptops, tablets or cell devices infected?

13. Any other equipment infected?

14. Action plan for removal.

15. Will infected devices be re-imaged or wiped before reconnection?

16. When was the last update of anti-virus signature files?

17. When was the last operating system update?

18. Was any CJIS data or personal identification information compromised?

19. The TLETS system will remain disconnected from TLETS until VIA information Technology department can guarantee your systems are free from virus infection.

20. Once free from infection and given clearance by the CJIS Security Group on-call person, the system can be reconnected to TLETS and NLETS.

.05 ***Account Management Process:*** All employees with access to Criminal Justice Information must be fingerprinted and pass a fingerprint based background check. Depending on the position, different training may be required. All employees are required to take Security Awareness Training within 6 months of being hired, and every 2 years thereafter. When an employee separates from the Agency, their ID is disabled. Employees' badge access is also disabled, and or keys are returned.

A. Adding an Omnixx Account

1. The department schedules an appointment for the employee to be finger printed by the Fingerprint Applicant Services of Texas (F.A.S.T.) Program

2. The department receives the employee's background results

3. TAC completes TCIC User Request Form, and emails to TCIC_Training@dps.texas.gov

B. Disabling a user account: TAC completes TCIC User Request Form, and emails to TCIC_Training@dps.texas.gov
NOTE: TAC has SAGY permissions to disable the account in Omnixx

C. Adding access to VISINET

1. TAC obtains TCIC/NCIC username from DPS

2. TAC Sends an E-Mail to Bexar County Sheriff's Office Communication Division with a request for user access.

3. Bexar County Sheriff's Office Communications Division issues a username and password for the employee.

D. Disabling access to VISINET: Upon termination of employee, TAC sends an E-Mail to the Bexar County Sheriff's Office Communications Division requesting cancellation of the employees access to VISINET

E. Adding access to the DPS Secure Site

F. Terminating access to the DPS Secure Site

Security Incident Response Team Contact List

[List all security members to include: LASO, TAC, IT staff and others as necessary.]

Name: Stephen Baker	
Title: Terminal Agency Coordinator (TAC)	
Work phone: 210-362-2439	Home phone: N/A
Mobile phone: 979-479-5158	Pager: N/A
Work email: Stephen.Baker@Viainfo.net	
Alternate email: N/A	

Name: George Aguilar	
Title: Local Agency Security Officer (LASO)	
Work phone: 210-362-2439	Home phone: N/A
Mobile phone: 210-380-8190	Pager: N/A
Work email: George.Aguilar@Viainfo.net	
Alternate email: N/A	

Name: Raul Botan – VIA Information Technology	
Title: IT Security Administrator	
Work phone: 210-362-2339	Home phone: N/A
Mobile phone: 210-823-7925	Pager: N/A
Work email: Raul.Botan@Viainfo.net	
Alternate email: N/A	

Name: Tina Saenz	
Title: DPS Rap back coordinator	
Work phone: 512-424-5105	Home phone: N/A
Mobile phone: N/A	Pager: N/A
Work email: tina.saenz@dps.texas.gov	
Alternate email: N/A	

TLETS SECURITY INCIDENT RESPONSE FORM

DATE OF REPORT: DATE OF INCIDENT:

REPORTING PERSON:

PHONE/EXT/E-MAIL:

LOCATION(S) OF INCIDENT:

SYSTEM(S) AFFECTED:

AFFECTED SYSTEM(S) DESCRIPTION (e.g. CAD, RMS, file server, etc.):

METHOD OF DETECTION:

NATURE OF INCIDENT:

INCIDENT DESCRIPTION:

ACTIONS TAKEN/RESOLUTION:

PERSONS NOTIFIED:

Copy to: Lt. Jeremy Klaus
Bexar County Sheriff’s Office – Public Safety Communications Manager
4700 Quarry Run
San Antonio, TX 78249
Office – 210-335-4601
JKlaus@Bexar.Org