Burleson Police Department
Administrative Policy and Procedures

Number: 02-002.5
Document Title: CJI Security
Effective Date: 03/17/2011
Last Revised Date: 1/18/2023
CALEA Standards Referenced: 11.4.4; 33.6.1a/b; 41.3.7a/b/c/d; 81.2.8; 82.1.1a; 82.1.6c/d

ISSUING AUTHORITY: Chief 01-18-2023
Billy Cordell, Chief of Police

I. **Purpose:**

This policy establishes guidelines for use and security of department issued equipment, Mobile Computer Terminal (MCT), workstations and related CJI information. Failure to comply with this policy can result in disciplinary action up to and including termination. All employees, contractors, and third party users are provided and required to review this policy. Burleson Police Department will protect the integrity of the CJI database and all data and information obtained using the MCT and/or hard-wired terminals by strictly following the procedures outlined in this directive.

II. **Definitions:**

A. CJI – Criminal Justice Information is the largest division of the United States Federal Bureau of Investigation, which was established in 1992.

B. MCT – Mobile Computer Terminal includes all computers that have access, via wireless or hardwired network to TLETS, TCIC, NCIC or any law enforcement database.

C. Secure Location – This includes the areas of the Burleson Police Department that are not open to the public and that have been properly marked by "Authorized Personnel Only" signs. This also includes official police vehicles that are locked and/or attended by authorized sworn personnel.

D. Non-Secure Location – This includes all locations not defined as "secured location" above.

III. **Procedures:**

A. All Police Department employees, contractors, support personnel, volunteers, janitorial staff, and anyone else who has unsupervised access to areas containing CJI equipment and data must have a fingerprint based records check conducted within 30 days of employment, appointment, or assignment.

B. Each person authorized to access TLETS, CJI data shall receive security awareness training within six months of appointment or employment and thereafter at least every two years in accordance with CJI policy. Training will be documented. The TLETS 16 and 40 hour training will count for this policy. [41.3.7a / 33.6.1a/b / 81.2.8]

C. Changes in authorized personnel will be immediately reported to TCIC training section within 24 hours. The terminated user's/contractor's accounts are disabled within 30 minutes of notification of termination. Annual user account validation audits will be completed and documented every year. All keys and access cards are confiscated or deactivated at the time of termination. [41.3.7a / 82.1.1a / 82.1.6c/d]

D. Visitors in secure areas will be escorted by authorized personnel at all times.

E. All printouts of CJI data shall be filed with the corresponding incident record or shredded. All secondary dissemination is signed for and reported to the TAC.

F. No CJI data will be saved to any external storing devices, USB, CD/DVD, floppy, internal or external hard drives or emails. [11.4.4 / 41.3.7c]

G. The department shall keep a list of all wireless device ID's and vendor telephone contact numbers so that devices can be promptly disabled, should the need arise.

H. CJI, TLETS, TCIC, and NCIC data shall be accessed only from secure locations as defined in definitions and used for law enforcement purposes only. [41.3.7b / 82.1.6c]

I. All doors to building or rooms that have CJI data are locked and posted as restricted areas stated in the definitions. All police vehicles containing CJI capable MCTs and the CJI network equipment server room shall be securely locked when not occupied by authorized personnel. [82.1.1a]

J. When transporting non-law enforcement personnel in police vehicles, caution should be used to prevent unauthorized viewing of CJI data from passengers. [82.1.1a]

K. Servers, PCs, and MCTs operating systems are supported by the manufacturer and maintained by the City's Information Technology (I.T.) department or contracted I.T. vendor. The operating systems are updated as released by the manufacturer. All MCT software will be current. [41.3.7d]

L. All equipment accessing CJI data shall have anti-virus software installed and updated daily. Network firewall equipment is not at end of life and updated as released by manufacturer. MCT's firewall shall be enabled at all times. All unused user or system accounts will be disabled. [82.1.1a] All vendor default passwords will be changed prior to the firewall going online. [41.3.7d]

M. Users are not to share user ID and/or passwords.

N. All interface passwords will meet CJI requirements:
   1. Passwords shall be a minimum length of eight (8) characters.
   2. Passwords shall not be a dictionary word or proper name.
   3. Passwords and the User ID shall not be the same.
   4. Passwords shall be changed within a maximum of every 90 days.
   5. All systems shall prevent password reuse of the last ten (10) passwords.
   6. Passwords shall not be transmitted in the clear outside the secure domain.
   7. Passwords shall not display when entered.

O. IOS/Firmware updates are installed as deemed appropriate and checked monthly by the city's I.T. department or contracted I.T. vendor. Firmware and software updates are downloaded to the server as soon as released by the manufacturer.

Workstations and MCTs are updated automatically. Virus protection is checked daily and updated as soon as released by the manufacturer. [41.3.7d]

P. All storage media containing or used for CJI data that is no longer used shall be secure-formatted using methodology that over-writes all data in three iterations meeting the Department of Defense standards. [82.1.1a]

Q. The agency will use a minimum of 128-bit AES encryption.

R. The agency will keep a log of the FIPS 140-2 certificates.

S. MCTs are either removed or disabled and secured by the officer when police vehicles are out of service and no longer on the police department property.[82.1.1a] That person will email the vehicle number to the group email, fleetpd@burlesontx.com, indicating that the vehicle is out of service.

T. The city's I.T. department will disable all network services not needed. A log is kept of allowed network services.

U. All users will lock or log off workstations upon departing the immediate area. (Ctrl + Alt + Delete, then lock or log off) [82.1.1a]

V. The law enforcement computer network shall be segmented in such a way as to prevent unauthorized access to CJI data. [41.3.7c / 82.1.1a]

W. Employees will not connect personal equipment to the internal network to access CJI data. [11.4.4 / 41.3.7c / 82.1.6c]

IV. **Reporting:**

A. It shall be the responsibility of each authorized user to report any violations of this CJI Security policy. In the event a violation or breach is detected, the reporting party will notify the Terminal Agency Coordinator (Communication Supervisor) and/or Local Agency Security Officer (Administrative Captain). They in turn will execute the Burleson Police Department CJIS Incident Handling and Response Plan (BPD 122-14) and notify appropriate DPS personnel and city I.T. staff. The city I.T. department will take appropriate action to isolate and eliminate the breach in security.

B. Any violation(s) of this policy shall result in disciplinary actions up to and including termination.