Burleson Police Department

Administrative Policy and Procedures

Number: 02-0025
Document Title: CJI Security
Effective Date: 03/17/2011
Last Revised Date: 09/07/2017
CALEA Standards Referenced:

ISSUING AUTHORITY: Chief B Polk 09.12.17

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.

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.

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.

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.

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.

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

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.

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. All vendor default passwords will be changed prior to the firewall going online.

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.