



Tulsa Police Department

This policy statement and the procedures thereunder are intended for Police Department use only. The policies, procedures, and regulations are for internal Police Department administrative purposes and are not intended to create any higher legal standard of care or liability in an evidentiary sense than is created by law. Violations of internal Police Department policies, procedures, regulations, or rules form the basis for disciplinary action by the Police Department. Violations of law form the basis for civil and/or criminal sanctions to be determined in a proper judicial setting, not through the administrative procedures of the Police Department.

Policy # 318B

Policy Name Criminal Justice Information Services

Approved by *Wendell Franklin, Chief of Police*

Effective Date 01/21/2016

Approved Date 01/21/2016

Previous Date NEW

PURPOSE OF CHANGE:

To update policy format.

POLICY:

It shall be the policy of the Tulsa Police Department to protect the integrity of the Criminal Justice Information Services (CJIS) database and all data and information obtained through use of MDCs and/or hard-wired OLETS terminals by strictly following the procedures outlined in this policy. Only authorized personnel will have access to OLETS. All employees authorized to utilize the system must comply with State Law and policy. Failure to comply with this policy can result in disciplinary action up to and including termination.

The department's participation in the OLETS system is conditional upon our adherence to policy as set out in the OLETS Operating Manual and applied through these guidelines. We are subject to audit by the DPS and/or FBI for compliance to all OLETS policies. The system is monitored periodically at the control point and violations of the adopted rules and regulations will result in corrective measures being taken against the offending agency. All employees with authorized OLETS access are reminded that the system is designed exclusively for use by criminal justice agencies in conducting their lawfully authorized duties within their respective jurisdictions and between agencies as required. Use of the system for any other purpose is a violation of State Statutes and Federal Regulations as well as a user agreement which could result in the termination of service to any agency found responsible for such offenses. Data stored, and information accessed through these terminals must be restricted to duly authorized criminal justice agencies or government agencies under the control of a criminal justice agency.

SUMMARY: Procedures for utilizing and protecting CJIS.

APPLIES TO: All police personnel

DEFINITIONS: See Policy 318A Attachment for definitions.

PROCEDURES:

1. CJIS, OLETS and NCIC data shall be accessed ONLY from secure locations, as defined in the attachment.
2. All Police Department employees, contractors, support personnel, volunteers, janitorial staff, and anyone else who has unsupervised access to areas containing CJIS equipment and data must have a fingerprint-based records check conducted within 30 days of employment, appointment, or assignment.
3. Each person authorized to access OLETS and CJIS 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. Training will be documented. The OLETS 16- and 40-hour training will count for this policy.
4. All doors to buildings or rooms that have CJIS data are locked and posted as restricted areas stated in the definitions. All police vehicles containing CJIS capable MDCs and the CJIS network equipment server room

shall be securely locked when not occupied by authorized personnel.

5. City of Tulsa Security maintains a list of agencies issued door access cards of authorized personnel with unescorted access into physically secure areas.
6. Lost or stolen door access cards will be reported to the employee's supervisor. The supervisor will notify City of Tulsa Security to have the access card disabled and a new card will be re-issued to the employee.
7. Visitors in secure areas will be escorted by authorized personnel at all times.
8. When transporting non-law enforcement personnel in police vehicles, officers will close the screen of the MDC or position it in a manner that will prevent unauthorized viewing of MDC data. OLETS terminal screens shall be positioned to prevent unauthorized viewing.
9. NCIC Criminal History records requested from Teletype will be viewed at PSC (printout or computer screen), or on Messenger Lite Terminals within TPD. The NCIC Criminal History print outs will not be included in any arrest packets.
10. Logs for NCIC Criminal History records must be kept at each PSC and Messenger Lite terminal. The officer or PSC operator providing the information must sign this log and document on the log how the printout/information was destroyed such as by shredding or closing of the terminal. After being viewed, the log will also be signed by the officer viewing the information. Each division will maintain copies of their logs at their division. Logs must be copied and sent to the CJIS Coordinator by the first of each month. The originals will remain with the terminal for one year and then be forwarded to the CJIS Coordinator at the end of each year by January 15 of the following year.
11. If a NCIC Criminal History is printed out and taken away from a terminal, it becomes the responsibility of the officer receiving the printout. It must be noted on the log the name of the officer taking the printout. That officer must then maintain a log of what happens with the printout, such as what date it was shredded.
12. 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.
13. Users are not to share user ID and/or passwords.
14. All users will lock or log off workstations upon departing the immediate area. (Ctrl + Alt + Delete, then lock or log off).
15. Within the department, only commissioned officers and other authorized persons will be allowed to request criminal justice information inquiries of any kind.
16. All OLETS passwords will meet CJIS requirements:



17. Requests from outside the department will be honored when the identity of the requestor can be verified as a commissioned officer, or other authorized person (probation officer, parole officer, judge, etc.) who is making the request for a criminal justice purpose. This request and verification must be documented before information can

be shared.

18. CJI data may be shared with agencies that have an MOU with the department. These MOUs will be reviewed as necessary such as updated CJIS requirements or a change in the head of the agency with the MOU.
19. Audio response terminals and radio devices, whether digital or voice, shall not be used routinely for the transmission of criminal history beyond that information necessary to affect an immediate identification or to ensure adequate safety for officers and the general public. When an officer determines there is an immediate need for this information to further an investigation or there is a situation affecting the safety of an officer or the general public, then details of the criminal history record information may be transmitted.
20. Police personnel will notify the Oklahoma Department of Public Safety when a police employee separates employment or changes assignments and access to OLETS is no longer necessary. Notification to discontinue OLETS access shall be documented on the Tulsa Police Exit Form by Police Personnel. Network accounts need to be disabled; keys, badges, and access cards used to access vehicles, buildings or secure doorways need to be obtained from employees. Laptops need to be confiscated.
21. The CJIS Security Program Work Group (CJIS Work Group) meets on a regularly scheduled basis to review any identified incidents that have occurred and recommend follow-up actions. In addition, the CJIS Work Group will review the applicable CJIS policies for TPD, Public Safety Communication (PSC) and City of Tulsa.

REGULATIONS:

1. All employees authorized to utilize the system must comply with State Law and policy. Failure to comply with this policy can result in disciplinary action up to and including termination.
2. No CJI data will be saved to any external storing devices, USB, CD/DVD, floppy, internal or external hard drives or emails. CJI data will not be transmitted on any mobile device such as mobile phones and tablets. CJI data/printouts will not be emailed.
3. Employees will not connect personal equipment to the internal network to access CJI data.
4. It shall be the responsibility of each authorized user to report any violations of this security policy up the chain-of-command and to the proper authorities.

REFERENCES:

318A, *Use of Departmental Computer Systems*
318Attachment, *Use of Departmental Computer Systems – Attachment*