2-9 USE OF COMPUTER SYSTEMS

Related SOP(s): None

2-9-1 Purpose

The purpose of this policy is to provide procedures for the proper use of Department computers and Criminal Justice Information Systems (CJIS).

2-9-2 Policy

The Department will comply with the City of Albuquerque's "Employee Code of Conduct" regarding technology systems and the FBI CJIS Policy. The Department will also:

A. Maintain proper licensing restrictions and requirements for all technology assets;

B. Coordinate all technology efforts including, but not limited to, the effective acquisition and implementation of all technology systems, system applications, and hardware components, under the direction of the Technical Services Unit (TSU); and

C. Manage data and systems in a secure manner that is responsive to evolving technology threats.

2-9-3 Definitions

A. Technology System

Any electronic device, to include personally owned devices. Examples include, but are not limited to, the following categories:

1. Computer system - Any computer including, but not limited to desktop Personal Computer (PC), laptop PC, Notebook PC, or tablet that runs Windows, Mac OS (OSX);

2. Mobile device - any cellular phone, smartphone, or tablet that runs an operating system, including, for example, Android or iOS; and

3. Personally owned device - Any device owned by an individual, not provided or managed by APD Tech Services.

B. CJIS

CJIS is the acronym for Criminal Justice Information Services. The full CJIS document is located on the FBI site at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

C. Criminal Justice Information (CJI)

The abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data is exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

D. Criminal History Record Information

Information on specific individuals relating to their recorded history of interactions with the criminal justice system including arrests, charges, detentions, and indictments.

E. Dissemination

The act of spreading criminal history record information, or the absence of criminal history record information, to any person or agency outside APD.

F. NCIC III (Triple-I)

The National Crime Information Center Interstate Identification Index, managed by the FBI and state law enforcement agencies.

G. TSU

The Technical Services Unit, commonly known as the APD Help Desk. The contact number is 768-2359.

H. Physically Secure Location

Any facility, criminal justice conveyance, area, room, or group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal

justice agency management control, State Identification Bureau (SIB) control, FBI CJIS Security addendum, or a combination thereof.

I. TAC - Terminal Agency Coordinator (TAC)

The point of contact for the New Mexico Department of Public Safety (NMDPS) and the Federal Bureau of Investigation (FBI) who ensures compliance with state and NCIC III policies and regulations. For more information on the TAC, please review the CJIS document (Section 3.2.3) or contact TSU.

2-9-4 Procedures

A. General Computer Use - Applicable to All Personnel

Department personnel:

1. Shall not disseminate or reveal any CJI without proper authorization.

2. Shall not use City computers, hardware, and/or software for any personal compensation or profit.

3. Shall access department records, systems, the Criminal Justice Information System, and the files located within CJIS only as permitted in the performance of official duties and for criminal justice purposes.

4. Shall not create or run unauthorized jobs, operate a computer in an unauthorized mode, or intentionally cause any kind of operational malfunction or failure.

5. Shall cooperate with the audit and/or investigation of any electronic device, to include personally owned devices. Any technology system used for work purposes is subject to audit and public information disclosure requirements.

B. Computer Training

1. Supervisors shall ensure that all of their employees have the training required to properly operate applications and comply with all relevant policies, rules, regulations, and statutes governing the security and dissemination of CJI.

C. Access - All Personnel

1. Personnel will be given the least possible access to computer systems according to their assignment, duties, and responsibilities, and follow CJIS requirements of the least possible access.

2. Personnel will comply with all application access rules.

3. Personnel must only use their own password or username to gain access to their designated systems.

4. Personnel will not lend their password or username to anyone.

5. Personnel will adhere to system procedural requirements as set forth within the application or the system user's manuals.

6. User passwords must be unique and follow the City of Albuquerque password guidelines.

D. Terminating Sessions

1. Personnel will lock or sign-off of the computer system they are using before leaving it unattended.

2. A session lock of no greater than 30 minutes will be enforced at the group policy level, as per CJIS.

E. Network-Connected Technology System

1. Personnel are required to contact the TSU if network-connected computer equipment needs to be installed or moved. This notification must occur one business day in advance of the move or installation.

2. Employees may access Department/City Of Albuquerque (COA) secured networks with personally owned technology systems, provided they follow city Bring Your Own Device (BYOD) policy and the following guidelines.

   a There shall be no reasonable expectation of privacy for any device connected to a City of Albuquerque networks, or any device used for city business.
   b Any personal device connected to the Department/COA network must have current and up to date city approved antivirus software.

F. Loading of Software on technology devices

1. To maintain support and licensing requirements, all personnel will contact the Technical Services Unit before installing software on any Department-owned device (e.g., smartphone, computer).

2. Personal software, games, or any software not related to city business will not be loaded on department-owned computers, cellphones, or smartphones. Violations will immediately be reported to a supervisor.

3. Department-owned software will not be removed from any Department-owned computer without prior approval from the Technical Services Unit.

4. TSU will maintain a list of approved software and applications. Applications on this list will be installed on employee's devices according to the employee's roles. TSU will work with Department command staff or designees to ensure that this list is reviewed regularly to meet the operational needs of employees.

G. Computer Files

1. Personnel shall encrypt data stored on removable storage devices (Such as, but not limited to, USB devices) unless the device is only used within areas of controlled access.

2. Personnel shall retain data in accordance with the COA and Department data and evidence retention schedules and policies.

3. Storage media shall be salvaged through TSU and TSU shall ensure that the data has been erased 3 times prior to being released or reused.

H. Security

All personnel shall:

1. Report violations, or suspected violations of this policy to their supervisor. The supervisor will inform either the TAC or TSU of the violations immediately.

2. Report any security breaches or suspected security breaches to their supervisor. The supervisor will inform either the TAC or TSU of the violations immediately.

3. Unless excepted by TSU, all technology devices shall be maintained by TSU with up to date versions of software (including software patches and bug fixes). Anti-virus software must be installed, running and up to date

4. Failure to report security violations or breaches may result in disciplinary action.

2-9-5 Use of Criminal Justice Information Services (CJIS)

The following section contains requirements specific to CJIS and may contain additional or overriding requirements to the previous sections of this policy. In the event of a conflict with non-CJIS sections of this document, this section will prevail.

A. Authorized User Access to CJIS

1. Only Department personnel or Department authorized agents may access CJIS information.

2. Information may be obtained from CJIS for authorized criminal justice purposes only, as determined by the Chief of Police.

3. Department personnel shall not use CJIS for personal use or non-law enforcement related activities.

4. Inquiries made for personal use, unauthorized use, or dissemination of the information may result in internal discipline, as well as penalties under federal and state law.

5. Inquiries through any CJIS, including, but not limited to, Motor Vehicle Division Database, NCIC III, NMLETS/NLETS inquiries to other jurisdictions, and LInX are only to be made for law enforcement purposes, as authorized by the APD.

6. Employees shall not discuss or provide CJIS information to any person who is not a member of the justice system without the permission of the Chief of Police or otherwise required by law.

7. Each user must use a unique password, change their password when prompted, and may not share passwords with other users.

8. All security training must be completed as required.

9. A Personally Owned Information System or a publicly accessed computer may not be used to access CJIS information.

B. Department CJIS Requirements

1. APD must remain in compliance with the NCIC User Acknowledgement or risk termination of one or more of the services provided.

    a The User Acknowledgement is the formal agreement between APD and the New Mexico Department of Public Safety (NMDPS).
    b This document acknowledges the standards established in the FBI's CJIS Security Policy.
    c The standards require accuracy, completeness, timeliness, and security in the dissemination and recording of information.

2. Violations of the rules, regulations, policies, or procedures developed by FBI and adopted by the NMDPS or any other misuse or abuse of the NCIC system may result in agency disciplinary measures and/or criminal prosecution. Disciplinary measures imposed by the NMDPS may include revocation of individual certification, discontinuance of system access to APD, or purging APD's records. Sanctions 1-7 may also be used.

3. Every user must have the least access to CJIS systems as possible.

4. Advanced authentication (e.g., 2FA) must be used wherever required by CJIS.

5. All technology services, including software and web services, must be registered with TSU before installation.

6. Antivirus software must be installed on every PC. Any security incidents must be reported to a supervisor.

7. All hardware purchases must be approved through TSU.

8. Maintaining security of the terminal sites and information received is the responsibility of agency personnel operating the terminal, the TAC, and the agency head. Terminal locations must be secure from unauthorized access, and all employees authorized to use the system shall be instructed on the proper use of the equipment and the dissemination of information received.

C. Rules Specific to NCIC

1. All employees shall adhere to the following NCIC policies:

    a All employees who use terminals that have access to information in NCIC files must be trained and certified to use NCIC.

b Any information obtained through these systems shall not be disseminated to unauthorized persons.
   i Examples of agencies, organizations, and persons to whom we cannot release criminal history information include passport agencies, CYFD, Adult Protective Services, Crimestoppers, victims, witnesses, families, and press.
c Inquiries into these systems shall not be made in response to a request by another criminal justice agency or by any retired employees.
d The NCIC III system shall only be used by personnel involved in criminal and background investigations.
e Any misuse of the NCIC III system must be reported to the TAC. The TAC shall report the misuse to the NMDPS, and the violator's chain of command.

2. Use of NCIC Interstate Identification Index (NCIC III) is regulated by the FBI and in accordance with the Code of Federal Regulations (28 CFR Part 20). Improper use of the system may result in severe penalties to APD and the individual user.

3. Printouts of criminal history record information from APD's computerized and manual files are prohibited except when:

a Required for the investigating officer's case file,
b Required by a prosecuting attorney,
c Required in a mutual criminal investigation with a court or government agency authorized to receive criminal history record information, or
d Authorized by a section or unit supervisor as required for an investigation or in an emergency.