2-9 USE OF COMPUTER SYSTEMS

Related SOP(s), Form(s), Other Resource(s), and Rescinded Special Order(s):

A. Related SOP(s)

3-41 Complaints Involving Department Personnel (Formerly 3-22 and 3-43)

B. Form(s)

None

C. Other Resource(s)

City of Albuquerque Bring Your Own Device (BYOD) Policy
City of Albuquerque Personnel Rules and Regulations, Section 301 Code of Conduct
City of Albuquerque Cybersecurity Policy
28 C.F.R. Part 20 Criminal Justice Information Services
Criminal Justice Information Services (CJIS) Security Policy
Inspection of Public Records Act of 1978

D. Rescinded Special Order(s)

SO 22-43 Amendment to SOP 2-9 Use of Computer Systems

2-9-1 Purpose

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

2-9-2 Policy

It is the policy of the Department to comply with the City of Albuquerque Personnel Rules and Regulations on Code of Conduct regarding technology systems and the Federal Bureau of Investigations (FBI) CJIS Security Policy.

N/A

2-9-3 Definitions

A. 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.

B. Criminal Justice Information Systems (CJIS)

A division of the FBI that administers Security Policy that contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI).

C. Criminal Justice Information (CJI)

An abstract term used to refer to all FBI CJIS-provided data necessary for law enforcement agencies to perform their mission and enforce laws, including but not limited to: biometrics, 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 are exempt from the protection levels required for CJI: transaction control type numbers (e.g., Origination Agency Identification (ORI), NCIC, FBI number (FNU), etc.) when not accompanied by information that reveals CJI or personally-identifiable information.

D. Dissemination

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

E. National Crime Information Center (NCIC) Interstate Identification Index (Triple I)

An electronic clearinghouse of crime data utilized by Department personnel to identify stolen property, Motor Vehicle Department (MVD) information, missing or runaway persons, and wanted persons of a nationwide interest.

F. Technical Services Unit (TSU)

The unit commonly known within the Department as the “APD Help Desk.”

G. Technology System

1. Any electronic device, including but not limited to:

   a. A Computer system: any computer, including but not limited to a desktop computer/personal computer (PC), laptop PC, Notebook PC, or tablet that runs on a Windows or Macintosh operating system (OSX);
   b. A Mobile device: any cellular phone, smartphone, or tablet that runs an operating system, for example, an Android or Apple operating system (iOS); or
   c. A Personally-owned device: Any computer system or mobile device owned by an individual, not provided or managed by Tech Services Unit personnel.

H. Terminal Agency Coordinator (TAC)

The point of contact for the New Mexico Department of Public Safety (NMDPS) and the FBI who ensures compliance with state and Triple I policies and regulations.

6 **2-9-4 Procedures**

A. General Computer Use

1. Technical Services Unit personnel shall:

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 TSU personnel; and
c. Manage data and systems in a secure manner that is responsive to evolving technology threats.

2. Department personnel shall:

a. Contact TSU personnel at (505) 768-2359 or APDHelpdesk@cabq.gov;
b. Be given access to Department records, systems, CJIS, and the files located within CJIS only as permitted in the performance of official duties and for criminal justice purposes; and
4 c. Cooperate with the audit and/or investigation of any technology system, including personally-owned devices that are used for work purposes subject to audit and public information disclosure requirements, consistent with the Inspection of Public Records Act.

3 3. Department personnel shall not:

a. Disseminate or reveal any CJI without proper authorization;
b. Use City-issued computers, hardware, and/or software, including computer applications that are hosted elsewhere, for any personal compensation or profit; or
c. Create or run unauthorized jobs, operate a computer in an unauthorized mode, or intentionally cause any operational malfunction or failure.

B. Computer Training

Supervisors shall ensure 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. Computer Access

1. Department personnel shall:

   a. Be given the least possible access to computer systems according to their assignment, duties, and responsibilities, and follow CJIS requirements using the least possible access;
   b. Comply with all application access rules;
5 c. Only use their own password or username to gain access to their designated systems;
   d. Adhere to system procedural requirements as set forth within the application or the system user manuals; and
   e. Ensure that user passwords are unique and follow City guidelines.

5 2. Department personnel shall not:

   a. Lend or share their password(s) or username(s) to anyone; or
   b. Use their City credentials (e.g. email address) for personal use, software, and/or services.

D. Terminating Sessions

1. Department personnel shall lock or sign-off of the computer system they are using before leaving it unattended.

2. TSU personnel shall enforce at the group policy level, consistent with CJIS, a session lock of no greater than thirty (30) minutes.

7 E. Network-Connected Technology System

1. Within five (5) business days in advance of the move or installation, Department personnel shall notify TSU personnel of any technology system connected to the network that needs to be installed or moved. Examples of such technology systems include but are not limited to:

   a. Network-connected computers;
   b. Multi-function printers (MFP);
   c. Smart thermostats; and
   d. Scanners.

2. Department personnel may access Department- or City-secured networks with personally-owned technology systems as long as they follow the City's 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 network.
   b. Any personal-owned device connected to the Department or City network must have current and up-to-date, City-approved antivirus software and must meet minimum operating system and security standards.

F. Loading of Software on Technology Systems

1. To maintain support and licensing requirements, Department personnel shall contact TSU personnel before installing software on any Department-owned technology system (e.g., smartphone or computer).

2. Department personnel shall not load personal software, games, or any software that is unrelated to City business on Department-owned computers, cellphones, or smartphones. Violations shall immediately be reported to a supervisor.

7

3. Department personnel shall not remove Department-owned software from any Department-owned computer without prior approval from TSU personnel.

4. TSU personnel shall maintain a list of approved software and applications. TSU personnel shall install software and applications on an employee's technology system according to the employee's roles.

5. TSU personnel shall work with Department command staff or their designees to ensure the list of approved software and applications are reviewed periodically to meet the operational needs of Department personnel.

G. Computer Files

1. Department personnel shall encrypt data stored on removable storage devices, including but not limited to a universal serial bus (USB) device, unless the device is only used within areas of controlled access.

   a. Department personnel may request TSU personnel to assist with encrypting data stored on removable storage devices.

2. Department personnel shall retain data in accordance with the City and Department data and evidence retention schedules and policies.

3. TSU personnel shall salvage removable storage media. TSU personnel shall ensure that the device is either erased one (1) time before release or reuse or is physically destroyed.

4. When using cloud services with City data, Department personnel shall be aware of what data types are being stored and who it is being shared with.

   a. CJIS data shall only be stored on approved cloud services and only shared with authorized individuals.

7

H. Security

1. Department personnel shall report violations or suspected violations of this Standard Operating Procedure (SOP) to their supervisor.

   a. The supervisor shall immediately inform either TAC or TSU personnel and the IAPS Division of the alleged policy violations consistent with SOP Complaints Involving Department Personnel.

2. Department personnel shall report any security breaches or suspected security breaches to their supervisor.

   a. The supervisor shall immediately inform TAC or TSU personnel of the alleged violations.

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

4. Unless an exception has been approved by TSU personnel, all technology systems shall be maintained by TSU with up-to-date software versions, including software patches and bug fixes. TSU personnel shall install anti-virus software and ensure it is running and up-to-date.

   a. If Department personnel notice that their Department-issued device is not up-to-date, they shall contact the TSU Helpdesk.

5 **2-9-5 Use of CJIS**

A. The CJIS may contain additional or overriding requirements. In the event of a conflict with sections of this SOP, the provisions in CJIS will prevail.

6 B. Authorized User Access to CJIS

1. Only Department personnel or Department-authorized agents shall access CJIS information.

2. Department personnel shall obtain CJIS information for authorized, criminal justice purposes only, as determined by the Chief of Police.

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

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

4. Inquiries through any CJIS, including but not limited to the Motor Vehicle Division Database, Triple I, New Mexico Law Enforcement Telecommunications Service (NMLETS/NLETS), inquiries to other jurisdictions, and Law Enforcement

Information Exchange (LINX) inquiries are only to be made for law enforcement purposes, as authorized by the Department.

5. Department personnel 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.

6. Department personnel shall complete all required security training.

7. Department personnel shall not use a personally-owned information system or a publicly-accessed computer to access CJIS information.

6

C. Department CJIS Requirements

N/A

1. The Department must remain in compliance with the NCIC User Acknowledgement or risk termination of one (1) or more of the services provided.

   a. The Chief of Police signs the User Acknowledgement, which is the formal agreement between the Department and the NMDPS.
      i. This document acknowledges the standards established in the FBI's CJIS Security Policy.
      ii. The standards require accuracy, completeness, timeliness, and security in the dissemination and recording of information.

N/A

2. Violations of the rules, regulations, policies, or procedures developed by the FBI and adopted by the NMDPS or any other misuse or abuse of the NCIC system may result in NMDPS disciplinary measures and/or criminal prosecution.

   a. Disciplinary measures imposed by the NMDPS may include revocation of individual certification, discontinuance of system access to Department, or purging Department's records.

3. Department personnel shall have access to CJIS systems according to their role.

7

4. Advanced authentication, such as the two-factor authentication (2FA) or multi-factor authentication (MFA), shall be used wherever required by CJIS.

5. Department personnel shall have TSU personnel register all technology systems, including software and web services, before installation or use.

6. TSU personnel shall install antivirus software on every Department-issued PC. Any security incidents must be reported to a supervisor.

7. All hardware purchases shall be approved through TSU and follow the City's Technology Review Committee (TRC) approval guidelines.

8. Department personnel operating the terminal, the TAC, and the Chief of Police shall be responsible for maintaining security of the terminal sites and information.

9. Department personnel shall secure terminal locations from unauthorized access. Department personnel who are authorized to use the system shall be instructed on the proper use of the equipment, and the dissemination of information received.

D. Rules Specific to NCIC

1. Department personnel certified to use the NCIC system shall adhere to the following NCIC policies:

   a. All employees who use terminals that have access to information in NCIC files shall be trained and certified to use NCIC;
   b. Any document obtained or generated through NCIC shall not be disseminated to unauthorized persons or agencies; and
      i. Examples of agencies, organizations, and persons who cannot receive any document obtained or generated through NCIC include but are not limited to:
         1. Passport agencies;
         2. New Mexico Children, Youth, and Families Department (CYFD);
         3. Adult Protective Services;
         4. Albuquerque Crime Stoppers Program;
         5. Victims;
         6. Witnesses;
         7. Families; and
         8. Media.
   c. Inquiries into these systems shall not be made in response to a request by another criminal justice agency or by any retired employees.

2. Use of the NCIC system is regulated by the FBI and shall be in accordance with Title 28 of the Code of Federal Regulations, Part 20 Criminal Justice Information Services. Improper use of the NCIC system may result in severe penalties the Department and the individual user.

   a. Consistent with FBI and NMDPS requirements, every five (5) years, the TAC shall perform a criminal background check on Department personnel who are certified to use the NCIC system.
   b. Any misuse of the NCIC system shall be reported to the TAC.
   c. The TAC shall report any misuse to the NMDPS and the Internal Affairs Professional Standards (IAPS) Division for investigation, consistent with SOP Complaints Involving Department Personnel (refer to SOP Complaints Involving Department Personnel for sanction classifications and additional duties).

N/A

3. Department personnel shall not:

   a. Disseminate or reveal any CJIS information without proper authorization;

b. Use City-issued computers, hardware, and/or software, including computer applications that are hosted elsewhere, for any personal compensation or profit;
c. Create or run unauthorized jobs, operate a computer in an unauthorized mode, or intentionally cause any kind of operational malfunction or failure; or
d. Directly contact a software vendor for assistance with Department-approved and Department-supported software.

4. Department personnel shall contact the Department's Tech Services Unit for assistance with Department-approved and Department-supported software.

5. Printouts of criminal history record information from the Department's computerized and hardcopy files are prohibited except when:

   a. They are required for the investigating officer's case file;
   b. They are required by a prosecuting attorney;
   c. They are required in a mutual criminal investigation with a court or government agency that is authorized to receive criminal history record information; or
   d. They are required by a section or unit supervisor because they are required for an investigation or during an emergency.