	ANDOVER POLICE DEPARTMENT GENERAL ORDER		Number: M1118
			Page: 1 of 13
			Distribution: All
Title: RECORDS - ADMINISTRATION		Section: Administration	
Issued: 02/14/2012	Effective: 02/22/2012	Revised: 02/22/2024	
Rescinds: All Previous		Amends: 02/09/2023	
CALEA References: LE 82.1.1 – 82.1.6, 82.3.1- 82.3.6 COM 6.1.4, 6.1.6, 6.7.1, 6.7.2, 6.7.3, 6.7.6, 6.8.5, 6.8.6			
KLEAP References: 20.1.1 – 20.1.5, 20.2.5			
Federal/State Statutes: KSA 38-2312, 45-215 – 45-223 (KORA)			
Review: Annual		Authority: Chief Buck Buchanan	

I. Purpose


The purpose of this General Order is to provide procedures for the administration of the department's Records Section.

II. Policy

The Central Records function is important to the effective delivery of law enforcement services. Therefore, it is the policy of the Andover Police Department to maintain records in a manner that accounts for privacy and security of its documents and ensures the accurate reporting of crime data.

III. Definitions

- A. Interstate Identification Index (III):** A national index of criminal histories maintained by the Federal Bureau of Investigation.
- B. Criminal History Record Information (CHRI):** Data initiated or collected by a criminal justice agency on a person pertaining to a reportable event. The term does not include:
 1. Data contained in intelligence or investigatory files or police work-product records used solely for police investigation purposes.
 2. Wanted posters, police blotter entries, court records of public judicial proceedings, or published court opinions.
 3. Data pertaining to violations of the traffic laws of the state or any other traffic law or ordinance, other than vehicular homicide; or
 4. Presentence investigation and other reports prepared for use by a court in the exercise of criminal jurisdiction or by the governor in the exercise of the power of pardon, reprieve, or commutation.
- C. Juvenile:** A person under the age of 18 years of age.

	<p style="text-align: center;">ANDOVER POLICE DEPARTMENT GENERAL ORDER</p> <p style="text-align: center;">Title: RECORDS - ADMINISTRATION</p>	Number: M1118
		Page: 2 of 13
		Section: Management

IV. Regulations


- A. Members shall not allow department records to be viewed, obtained, or otherwise disseminated outside of the department except for those records disseminated in accordance with this General Order [D].
- B. Members will only print records from RMS for official business only [C].
- C. Members who print records from RMS shall shred the record when its use for official business is no longer needed [C].
- D. Members will not disseminate III, TLO, LEADS, or FLOCK information or otherwise use the information for anything other than approved department business [E]. In addition to department discipline, members violating this regulation may be criminally prosecuted.
- E. Members will not release Interstate Identification Index (III) information to outside agencies [C].
- F. Members will not allow another person to use their assigned SecurID token to access the KCJIS system [C].
- G. No criminal history information will be disseminated over the telephone unless the department member can ensure that the receiver of the information is authorized to obtain the information disseminated [C].

Rev. 02222024

V. Procedures

A. Responsibilities

1. The Communications Director is responsible for the overall operations of the E-911/Communications Section. Responsibilities of the function include:
 - a. Collection, compilation, maintenance, and distribution of all offense reports, arrest reports, citations, and other reports generated by the department;
 - b. Maintenance of the department's Records Management System (RMS) and Computer Aided Dispatching (CAD) systems;
 - c. Dissemination of information as authorized by statute;
 - d. Communication between the various departmental divisions and the public, providing information and coordination as appropriate;
 - e. Distribution and tracking of subpoenas;
 - f. Maintenance of arrest warrant files;
 - g. Maintenance of a Criminal History Record Information dissemination log;
 - h. Records pertaining to property obtained by the department pursuant to General Order O2110 Property Management.
2. The department will maintain, at a minimum, the following records:
 - a. Service calls and crimes by type (LE 82.3.2a);
 - b. Service calls and crimes by location (LE 82.3.2b);


	<p style="text-align: center;">ANDOVER POLICE DEPARTMENT GENERAL ORDER</p> <p style="text-align: center;">Title: RECORDS - ADMINISTRATION</p>	Number: M1118
		Page: 3 of 13
		Section: Management

Rev. 02222024


- c. Stolen, found, recovered, and evidentiary property files (LE 82.3.2c);
 - d. Traffic collision data (LE 82.3.3a);
 - e. Traffic enforcement data (LE 82.3.3b);
 - f. Roadway hazard information (LE 82.3.3c).
3. The following department functions may be permitted to maintain the listed records in a secure manner outside of the records area (LE 82.3.5):
 - a. Office of the Chief of Police
 - i. Records pertaining to internal affairs investigations;
 - ii. Pre-employment investigation records;
 - iii. Police vehicle accident records.
 - b. Special Services Division
 - i. Training records.
 - c. Operations Division
 - i. Records pertaining to use of force incidents;
 - ii. Records pertaining to police pursuits.
 - d. Investigations Section
 - i. Records pertaining to confidential informants;
 - ii. Intelligence records.

B. Security and Access (LE 82.1.1a, 82.1.1b; COM 6.7.1a, KLEAP 20.1.1c)

1. Physical access to secure areas of the department, including records storage and work area is controlled by key cards. Key cards are issued to department personnel and programmed to allow unaccompanied entry for authorized personnel. The IT Director will program and issue key cards to department members with appropriate access permissions.
2. Access to electronic records is controlled by usernames and passwords. Usernames and initial passwords are issued to authorized personnel by the IT Director for access to the department's secure network, and usernames and initial passwords are issued by the Records/Evidence Custodian to authorized personnel for access to the department's RMS. RMS can only be accessed by first accessing the department's secure network.
3. The department's records are stored within the secure area of the building. Physical records are kept locked and access is limited to Communications/Records personnel.
4. The following positions are authorized unescorted entry into the records area for duty-related purposes.
 - a. All department personnel;
 - b. Municipal Court personnel;
 - c. Authorized maintenance personnel, city employees, interns, and others who have passed an approved fingerprint-based KCJIS background check and

	<p>ANDOVER POLICE DEPARTMENT GENERAL ORDER</p> <p>Title: RECORDS - ADMINISTRATION</p>	Number: M1118
		Page: 4 of 13
		Section: Management


- signed an appropriate awareness statement;
- d. Clearly identified sworn officers of other agencies.
5. Unless otherwise authorized, any person who has not passed a fingerprint-based background check, must be escorted or monitored including elected officials, city employees, and private citizens.
6. Physical records may be obtained 24 hours per day through the on-duty Communications Officer.
 - a. Officers who need records will request the record from the on-duty communications officer. If the requesting officer is removing the record from the records area, the requesting officer will sign and date the Case File Checkout Log (APD Form 48) and write the purpose for obtaining the record. The on-duty Communications Officer will also sign and date the Case File Checkout Log.
 - b. When the record is returned, the returning officer will provide the record to the on-duty Communications Officer. Both the returning officer and the Communications Officer will document the return of the record on the Case File Checkout Log.
 - c. Records that are removed from the records area will also be documented in RMS as directed by the Records/Evidence Custodian by the Communications Officer before the end of their shift.
 - d. Monthly, the Communications Director will audit the Case File Checkout Log and RMS to ensure the provisions of this General Order are being followed.
7. Electronic records may be accessed 24 hours per day by members authorized to access RMS.
 - a. Officers may print records from RMS for official business only; however, printed records shall be shredded once the record is no longer needed for official business.
 - b. RMS automatically maintains a log of all printed records. The log will be reviewed following any event where the unauthorized release of records occurs or is suspected of occurring and members who have printed the questioned record may be held accountable for its unauthorized release in accordance with department General Orders.
8. The department uses electronic ticketing as its primary method for issuing citations for parking, traffic, and criminal violations and warnings.
 - a. Electronic tickets are only generated by the software and issued to officers as needed and when approved by a supervisor (LE 82.3.4a, KLEAP 20.2.5a).
 - b. Each electronic ticket issued has a unique, system-generated number that is tracked by the software from the point of generation to the point of being served to a violator (LE 82.3.4b, KLEAP 20.2.5b).
 - c. Security and access control to the electronic ticketing system, both the handheld devices and the systems database, is controlled through the use

	<p>ANDOVER POLICE DEPARTMENT GENERAL ORDER</p> <p>Title: RECORDS - ADMINISTRATION</p>	Number: M1118
		Page: 5 of 13
		Section: Management

of usernames and passwords that are unique to the individual authorized user. Except for the copy printed and issued to the violator, each electronic ticket remains in its electronic form within the secure system throughout its life cycle (LE 82.3.4c, KLEAP 20.2.5c).


C. Release of Agency Records (LE 82.1.1c, COM 6.1.4, 6.7.1b, KLEAP 20.1.1d)

1. Criminal history information including offense reports, most documentation associated with criminal cases, arrest data, and a multitude of other information gathered and stored by the department is restricted and may not be routinely disseminated to persons or agencies without a criminal justice interest. However, a legitimate, lawful request for a copy of a report will be honored in keeping with the spirit of the Kansas Open Records Act (KORA).
 - a. Criminal justice agencies are allowed access to Criminal History Record Information (CHRI). The following agencies are routinely authorized access to adult and juvenile records and dispositions, if available:
 - i. Any law enforcement agency, to include federal law enforcement agencies and those from other states;
 - ii. Office of Personnel Management (Federal Government Agency);
 - iii. Defense Security Service (Federal Government Agency);
 - iv. Office of the Butler County Attorney;
 - v. Butler County District Court;
 - vi. Andover Municipal Court;
 - vii. Andover Municipal Prosecutor;
 - viii. Adult Community Corrections;
 - ix. Juvenile Justice Authority;
 - x. Department for Children and Families (DCF);
 - xi. State and Federal Parole Officers.
 - b. Organizations, other than those mentioned above, that routinely request criminal history information in the course of employment background checks and other similar inquiries will first complete a non-disclosure agreement. Once the agreement is signed by the authorized signatories, that agency may receive the specified criminal history information. Such agreements are maintained by the Records/Evidence Custodian.
 - c. Individuals may request information, to include criminal history material. Generally, this material is limited to pages clearly labeled "Open Public Record" and any witness statements written by the person making the request. Requests should be made in writing using APD Form 58 and with the exception of motor vehicle accident reports, will be reviewed by the Records/Evidence Custodian, who will determine the appropriateness of the release of the requested information. If it is determined the information


	<p style="text-align: center;">ANDOVER POLICE DEPARTMENT GENERAL ORDER</p> <p>Title: RECORDS - ADMINISTRATION</p>	Number: M1118
		Page: 6 of 13
		Section: Management

may be released as a matter of public record, the appropriate copy and research fees will be paid before the material is released. Exception to the requirement for APD Form 58 will be made for insurance companies and agencies working on behalf of insurance companies requesting copies of motor vehicle accident reports. If release of the requested information is not approved, the requester will be notified in writing. In the absence of the Records/Evidence Custodian all open public record requests, with the exception of motor vehicle accident reports, will be forwarded to the Communications Director for review and assignment.

- d. All requests for information/reports will be scanned and entered into RMS under the appropriate incident number, and then forwarded to the Records/Evidence Custodian who will maintain a file of all Open Records/Information Requests. Any Open Records/Information requests that do not pertain to an incident report will also be filed in the Open Records/Information Request file.
- e. Certain agencies will send a representative to the department to obtain criminal history information. At this time, the representative must show their credentials to the Communications Officer before the check is performed. Using the guidelines above, a records check may or may not be performed. When records personnel receive a lawful request for a copy of a report, it will be honored in accordance with the Kansas Open Records Act (KORA).
- f. No Criminal History Record Information (CHRI) will be disseminated via wireless telephone, email, radio, or pager unless necessary to protect the safety of the receiving officer. The following methods for transmittal of requests for records may be utilized:
 - i. U.S. Mail.
 - ii. Fax (When the receiving person is standing at the fax machine to receive the information).
 - iii. Teletype.
 - iv. Personal Service.
- g. An individual may review and challenge their record as it is on file with the department under the Kansas Administrative Regulations (KAR) 10-13-1.
 - i. All such requests must be in writing and accompanied by a non-refundable fee of \$10.00.
 - ii. The requester must provide sufficient identification and state the reason for the review/challenge.
 - iii. Upon completion of the above requirements, the existing criminal record may be shown to the requester.
 - iv. Desired changes to the record must be submitted in writing.

	<p>ANDOVER POLICE DEPARTMENT GENERAL ORDER</p> <p>Title: RECORDS - ADMINISTRATION</p>	Number: M1118
		Page: 7 of 13
		Section: Management


- v. The department shall have 30 calendar days to answer the records challenge.
 - vi. The change request shall be forwarded to the Records/Evidence Custodian who will recommend a course of action and forward the request through the chain of command to the Chief of Police.
 - vii. Upon completion of the challenge and review, all documents associated with the review and challenge shall be scanned into the requester's RMS file.
2. Interstate Identification Index (III) and KBIQ (LE 82.1.7)
- a. Inquiries into the Interstate Identification Index (III) and KBIQ and their subsequent use are restricted by the department to conduct criminal investigations, background checks of employees and prospective employees or people receiving firearms in the possession of the department, and record entry purposes into NCIC. III and KBIQ data must be kept secure and confidential at all times.
 - b. In addition, the department prohibits the subject of the III and KBIQ records from reviewing their own record. Record requests of this nature shall be submitted in writing to the FBI Identification Division or the state of record.
 - c. The Kansas Criminal Justice Information Sharing (KCJIS) system (Open Fox) may be utilized to make an inquiry of the III and KBIQ databases. A user must possess a uniquely assigned security token and follow specified procedures for access to the system in order to obtain a III and KBIQ inquiry. Guidelines for completion of III and KBIQ inquiries may be accessed by authorized users on a secured website at <http://www.kcjis.state.ks.us>.
 - d. Members will shred III and KBIQ data when the data is no longer needed.
 - e. Communication Officers will log all III's and KBIQ reports ran at the request of officers, as well as, maintain a Secondary Dissemination Log. An officer requesting and receiving a III/ KBIQ Report will advise the Communications Officer of the status of the report after said officer has reviewed it. Example: Stored in the Case Jacket, stored in the applicant file, destroyed, etc. After the officer advises the status of the III/ KBIQ Report, the Communication Officer will log the status of the III or KBIQ in the Secondary Dissemination Log. If at any time the status of the III or KBIQ is changed, the office responsible for the change in status will advise the on-duty Communications Officer of the new status and the on-duty Communications Officer will document the change on the Secondary Dissemination Log. A printed III or KBIQ will not be removed from the building or otherwise disseminated in its original form.
 - f. Any time confidential information is removed from an III or KBIQ and placed in any documentation that leaves the Police Department's building, a Secondary Dissemination Log entry will be made. This includes, but is not

	<p style="text-align: center;">ANDOVER POLICE DEPARTMENT GENERAL ORDER</p> <p style="text-align: center;">Title: RECORDS - ADMINISTRATION</p>	Number: M1118
		Page: 8 of 13
		Section: Management

limited to, any information removed from the III/KBIQ and placed on an affidavit. It is the dissemination officers' responsibility to advise Communications/Records of all aspects in the Secondary Dissemination including, but not limited to, Subjects Name, Race, Sex, DOB, Subjects SID Number or FBI Number; Name, Rank/Title of person whom the record was given; type of data disseminated, and officer's name making the dissemination.

D. Juvenile Records

1. The following Juvenile records and reports, if maintained by the department, will be readily distinguishable in a manner approved by the Communications Director (LE 82.1.2a, KLEAP 20.1.1a):
 - a. When a juvenile is the victim of abuse or neglect;
 - b. When a juvenile has been the victim of a sex crime;
 - c. When a juvenile is a suspect or has been taken into police custody;
 - d. When a juvenile is a child in need of care, including runaway or truant;
 - e. When a juvenile is a status offender (e.g. curfew violation, possessing or consuming alcohol, cigarette violations, which if committed by an adult would not be a crime); and
 - f. Juvenile identification documents including fingerprints, photographs, and other forms of identification.
2. Fingerprints, photographs, and other forms of identification will be collected pursuant to General Order O2502 Juvenile Operations (LE 82.1.2b, KLEAP 20.1.1b).
3. Section B – Security and Access of this General Order will apply to juvenile confidential information (LE 82.1.2c).
4. Disposition of records pertaining to juveniles that have reached the age of 18 will be in accordance with the Record Retention Schedule of this General Order (LE 82.1.2d).
5. Expungement and/or destruction of juvenile records is accomplished in accordance with KSA 38-2312. In all juvenile matters, the department will adhere to all court orders demanding expungement/destruction of juvenile arrest records specifically and exactly as issued by a court of jurisdiction. Upon receipt of an expungement order the following procedures will be adhered to (LE 82.1.2e):
 - a. All storage locations (physical and electronic) are searched for reports and records concerning the subject of expungement.
 - b. Once the reports and records are located, they are marked in RMS as expunged, access is limited to the Communications Director and Records/Evidence Custodian, and the expungement order is attached to the


	<p style="text-align: center;">ANDOVER POLICE DEPARTMENT GENERAL ORDER</p> <p style="text-align: center;">Title: RECORDS - ADMINISTRATION</p>	Number: M1118
		Page: 9 of 13
		Section: Management

RMS file. Physical files not already in RMS will be digitized, entered into RMS, and treated as outlined above. The physical file will be shredded.

- c. A review of the files will be completed by the Communications Director to ensure the expunged file is not accessible to others within the department.
- d. A Communications Officer assigned by the Communications Director will attempt to review the expunged file to ensure the file has been sequestered in accordance with this General Order.

E. Retention Schedule (LE 82.1.3, COM 6.7.2, KLEAP 20.1.2)

1. All documents considered to have some evidentiary value will be stored in evidence pursuant to General Order O2110 Property Management.
2. Videotapes taken at a crime scene will be transferred from the camera into the department's RMS.
3. The indicated department records will be retained in an appropriate location according to the following schedule:
 - a. Accident Reports: A minimum of ten calendar years
 - b. Adult Arrest Reports: A minimum of five calendar years for misdemeanor arrests and a minimum of 20 calendar years for felony arrests.
 - c. Adult Criminal Reports: A minimum of five calendar years in misdemeanor cases and a minimum of 20 calendar years for felony cases.
 - d. Juvenile Arrest Reports: Retain at a minimum until the age of majority is reached.
 - e. Juvenile Criminal Reports: Retain at a minimum for five calendar years past adjudication.
 - f. Information or Documentation Reports: Retain at a minimum for three calendar years.
 - g. Adult Fingerprint Cards: Retain until submitted to the State Central Repository.
 - h. Juvenile Fingerprint Cards: At a minimum retain until submitted to the State Central Repository or five calendar years past the age of majority.
4. Following the expiration of the above retention periods, the original documents may be removed from the storage location and shredded by authorized personnel. Electronic files are retained indefinitely and are not subject to destruction unless otherwise indicated by this General Order (COM 6.8.6d).
5. The department will adhere to all court orders demanding expungement/destruction of department records, specifically and exactly as issued by a court of jurisdiction. Upon receipt of an expungement/destruction order, the following procedures will be adhered to (LE 42.1.3):
 - a. All storage locations (physical and electronic) are searched for reports and records concerning the subject of expungement/destruction.

	<p style="text-align: center;">ANDOVER POLICE DEPARTMENT GENERAL ORDER</p> <p>Title: RECORDS - ADMINISTRATION</p>	Number: M1118
		Page: 10 of 13
		Section: Management


- b. Once the reports and records are located, they are marked in RMS as expunged, access is limited to the Communications Director and Records/Evidence Custodian, and the expungement order is attached to the RMS file. Physical files not already in RMS will be digitized, entered into RMS, and treated as outlined above. The physical file will be shredded.
- c. A review of the files will be completed by the Communications Director to ensure the expunged file is not accessible to others within the department.
- d. A Communications Officer assigned by the Communications Director will attempt to review the expunged file to ensure the file has been sequestered in accordance with this General Order.

F. Collection and Submission of Crime Data (LE 82.1.4; COM 6.7.3, KLEAP 20.1.3)

1. The Communications Director, or a designee, will extract incident-based crime information from RMS for reporting as required by the Chief of Police, the Kansas Bureau of Investigation, and the Federal Bureau of Investigation.
2. After a report has been submitted and approved, the pertinent data will be submitted to the Kansas Incident Based Reporting System (KIBRS). Only those crimes listed as Group A or Group B offenses as outlined in the KIBRS operating manual will be submitted.
3. Prior to submitting the data the Communications Director or a designee will reconcile data to correct inconsistencies.

G. Report Accounting System (LE 82.1.5)

1. All events reported to the department through the Communications Division will be assigned a unique CAD number by the Computer Aided Dispatch (CAD) computer. In addition to the CAD number, state reportable incidents and any event requiring documentation will be assigned a unique case number by CAD (COM 6.7.6, KLEAP 20.1.4a).
2. At the start of each business day, the Records/Evidence Custodian or a designee identified by the Communications Director will generate a list of case numbers assigned the previous day(s) and compare the list to cases entered into RMS. Discrepancies between the list and reports entered into RMS will be reported to the appropriate Division Commander.
3. All reports and supporting documents are filed within RMS in numerical order according to the case number, and names of involved parties are stored alphabetically in a master name index (LE 82.3.1, KLEAP 20.1.4b).
4. All persons entered into RMS will automatically be assigned a unique number and all subsequent entries and information concerning that person will reference that number, including arrest records such as photographs (if taken locally) and arrest reports (LE 82.3.6).

	<p style="text-align: center;">ANDOVER POLICE DEPARTMENT GENERAL ORDER</p> <p style="text-align: center;">Title: RECORDS - ADMINISTRATION</p>	Number: M1118
		Page: 11 of 13
		Section: Management


- a. Fingerprints collected and submitted electronically will be available through the Kansas Bureau of Investigation. Fingerprints collected using ink will only be kept until submitted to the Kansas Bureau of Investigation.
 - b. Booking photographs taken at the Butler County Jail will be available from the Butler County Jail when requested.
5. All documents considered to have some evidentiary value will be placed into evidence pursuant to General Order O2110 Property Management.
6. Section and Division Commanders are responsible for ensuring follow-ups are completed pursuant to General Order M1108 Victim-Witness Assistance, as well as any other supplemental reports, and the follow-up reports are properly submitted into RMS (KLEAP 20.1.4c).

H. Security of RMS


1. Access to RMS is restricted to authorized department members as previously outlined in this General Order. Access restriction is ensured by the issuance of unique usernames and passwords for both the department's secure network and for RMS, which is located within the secure network (LE 82.1.6c; COM 6.8.6a, KLEAP 20.1.5c).
2. Servers and network equipment are secured in a limited access room onsite and RMS data is backed up to a secure, off-site location daily (LE 82.1.6a&b; COM 6.8.6b&c, KLEAP 20.1.5a & b).
3. The Communications Director, or designee, will request from the IT Director quarterly audits of usernames and passwords. After a review of the audit, the Communications Director shall submit a report regarding the outcome of the audit to the Chief of Police (LE 82.1.6d; COM 6.8.5, KLEAP 20.1.5f).

I. Security of Computerized Criminal History Records

1. The department accesses a variety of criminal justice information systems through state and national computer switches. These systems include:
 - a. Automated Statewide Telecommunications and Records Access (ASTRA), which provides access to the following information sources:
 - i. National Law Enforcement Telecommunications System (NLETS);
 - ii. National Crime Information Center (NCIC);
 - iii. Automated Law Enforcement Response Team (ALERT);
 - iv. Interstate Identification Index (III);
 - v. Motor vehicle registration records;
 - vi. Driver's license records.
 - b. Kansas Criminal Justice Information Systems (KCJIS) provides access to the following information sources:
 - i. Kansas Criminal History Record Information (CHRI);

	<p>ANDOVER POLICE DEPARTMENT GENERAL ORDER</p> <p>Title: RECORDS - ADMINISTRATION</p>	Number: M1118
		Page: 12 of 13
		Section: Management

- ii. Officer Safety Information;
 - iii. Methamphetamine case tracking;
 - iv. Master Name Index (MNI) search;
 - v. National Crime Information Center (NCIC);
 - vi. National Law Enforcement Telecommunications System (NLETS);
 - vii. Kansas Department of Revenue.
2. In order to access the information systems listed above the following conditions must be met:
- a. Computers that provide access to information systems shall be physically secure from unauthorized personnel. Access to an area in which a terminal is located is restricted to employees of the department or those under escort by an employee of the department.
 - b. All personnel who access the referenced systems must satisfactorily complete a fingerprint-based background check.
 - c. All NCIC operators shall be trained in accordance with NCIC policy and tested to affirm proficiency within six months of assignment to such position. Following initial certification, operators will be retrained and retested biennially.
 - d. All personnel will receive KCJIS Security Awareness training every two years.
 - e. All personnel authorized access to the referenced information systems may be issued a SecurID token.
 - i. The Department's Terminal Agency Coordinator (TAC) is responsible for maintaining a list of members who are assigned a SecurID token and which token they are assigned.
 - ii. KCJIS users shall be authenticated by means of a unique user ID, Personal Identification Number (PIN), and password. The password is the six characters displayed on the SecurID token. The PIN and the password together make up the passcode. Employees are responsible for the establishment of the PIN.
 - iii. Upon termination or separation from service employees will return their assigned SecurID token to the TAC. The KBI will be notified of the separation and the issued token will be deactivated as soon as possible.
 - iv. Any authorized KCJIS user who needs to access KCJIS at a time when their token is not functioning or is unavailable may obtain a temporary password from the KBI. The password is only valid during the user's shift.
 - v. Lost tokens shall be immediately reported to the KBI and the Records/Evidence Custodian so that it may be deactivated to prevent unauthorized access to KCJIS.
3. If an incident occurs where CJIS information was misplaced, lost, or stolen (KLEAP 20.1.5e):

	<p style="text-align: center;">ANDOVER POLICE DEPARTMENT GENERAL ORDER</p> <p style="text-align: center;">Title: RECORDS - ADMINISTRATION</p>	Number: M1118
		Page: 13 of 13
		Section: Management

Rev. 02222024

- a. Immediately inform your supervisor;
 - b. Contact the Communications Director via email with a detailed description of the information that was released, and;
 - c. On the next business day, the Communications Director and/or the agency LASO will complete a security incident notification and contact the Kansas Highway Patrol on behalf of the agency.
4. If a terminal with CJIS access is suspected of having a virus:
- a. Unplug the network cable and/or disable Wi-Fi;
 - b. Leave any antivirus notices on the screen;
 - c. Inform your supervisor and notify the Communications Director via email, and;
 - d. Contact the I.T. Help Desk via email with a detailed description of the incident.
5. I.T. will walk through instructions on resolving the issue if they are not available to come to your location. Tracking and documenting will be accomplished by reviewing the log file after the incident. Once I.T. has been notified and the situation has been identified/handled, the Communications Director will contact the Kansas Highway Patrol on behalf of the agency.

Rev. 02222024

J. Security and Disposal of Work-Sensitive Documents (COM 6.1.6)

1. All department personnel are responsible for the security of work-sensitive documents in their possession.
2. Work-sensitive documents include, but are not limited to:
 - a. Information obtained from TLO/NCIC/FLOCK/LEADSONline;
 - b. Work notes containing event information;
 - c. Crime analysis documents;
 - d. Watch Summaries; and
 - e. Other documents containing incident, victim, witness, suspect, or personal information.
3. At the end of each shift, all department personnel must destroy or render unreadable all transient work-sensitive documents that are no longer needed and not subject to retention according to the Department's Records Retention and Disposition. Transient work-sensitive documents include, but are not limited to:
 - a. Call taking notes;
 - b. TLO/NCIC/FLOCK/LEADSONline printouts; and
 - c. Any other computer printouts containing incident, victim, witness, suspect or personal information.