Colorado Springs Police Department
General Order

1612 Records Security

Section 1600 – Information Systems & Police Records

Effective Date: 5/5/2025
Supersedes Date: 5/8/2024

.01 Purpose

The purpose of this directive is to set policy and guidelines for ensuring the security and confidentiality of the department's criminal records.

.02 Cross Reference

GO 1606 Criminal Records Information
GO 1618 Juvenile Records
GO 1690 Public Information Office and News Media

.03 Discussion

The department has a responsibility to ensure the confidentiality and security of departmental records. To fulfill this responsibility, procedures are maintained in the SOP of the Records Section that: limit access to records; control additions or deletions of data; ensure authorized distribution; and provide for screening and training personnel directly involved in the records system. These procedures protect the public, the city, and the department from unauthorized release of criminal records information.

.04 Policy

All department personnel will take proactive steps to ensure the security and confidentiality of criminal offense records and the information they contain.

Employees will not use their position to gain access to any department record, hard copy or electronic, for personal use or commercial gain. Violations will be grounds for disciplinary action.

CSPD officers, detectives, CSOs, and civilian investigators are not permitted to permanently store any digital evidence, case investigative information, and data containing personally identifiable information (PII) outside of department authorized locations.

CSPD personnel are not permitted to store original or paper copies of case investigative information, and data containing personally identifiable information (PII) outside of official channels, or authorized locations.

.05 Definitions

Case Information: Any information gathered on a person or group of people regardless of whether or not a formal case report was initiated.

Personal Use: Viewing of records solely to satisfy personal curiosity unrelated to any official department purpose.

Records Custodian: The Records Manager of the Records Section is designated as the official Custodian of Records of the Colorado Springs Police Department.

Records: Documents, electronic media, Body Worn Camera footage, audio and video records, or other memorialization of official action taken by the Colorado Springs Police Department.

.10 Release of Records

Department personnel are not authorized to release records to members of the public without deconflicting the release with the Records Section. This is to protect the confidentiality and security of our records, and to ensure compliance with law and policy that seal or otherwise restrict the release of many criminal justice records produced or held by CSPD.

This restriction does not apply to records not subject to sealing that are released by the Strategic Initiatives Section, the Crime Analysis Section, the Public Affairs Section, or the CSPD Public Safety Attorney in the course of their business. It also does not apply to information shared between CSPD and other criminal justice or law enforcement agencies, during discovery to prosecutorial agencies or the City Attorney's Office, or as otherwise required by law.

There are no restrictions for releasing records to the City Attorney's Office, District Attorney's Office, or other prosecutorial agencies when those requests are for official business (e.g., case discovery, lawsuit preparation, etc.).

.11 Access to Records Area

Entrances to the Records Section shall be monitored by all Records personnel to ensure that unauthorized personnel are not allowed access to the section. Access to the Records area is limited, exclusively, to personnel assigned to the Records Section and to persons specifically authorized access by the Office of the Chief of Police or by the Records Manager or their designee.

.16 Receiver

Department personnel receiving criminal history information, offense reports, or any other departmental records will safeguard the information so that further dissemination is limited to those authorized to receive it.

.20 Records Information from NCIC/CCIC

Criminal history information obtained from the NCIC/CCIC systems, or any such information obtained through an automated system that connects with those systems, will be released only to criminal justice agencies and criminal justice personnel, and then only by authorized Records Section personnel.

Motor vehicle registration and owner information obtained from CCIC may be accessed by any department officer or other authorized CSPD employee who requires the information to fulfill an official governmental function.

.22 Automated Systems Security

All automated systems terminals will be located in areas that are secure and accessible only to personnel authorized to operate them in accordance with rules established in the FBI CJIS Security Policy Manual.

Information obtained from local, state, or federal automated systems will not be released to anyone except department personnel and those authorized by the Office of the Chief of Police, the Records Manager and as allowed under the Colorado Open Records Act, the Colorado Criminal Justice Records Act and Children's Code Records and Information Act. Such information includes motor vehicle registration records, drivers' license information, stolen property information, any information contained in a local, state, or federal automated system, and various other records held by CSPD.

.24 Criminal Record Checks

Federal laws governing NCIC and CCIC require that all criminal history checks be stamped confidential, receipted, and entered on a criminal history log sheet. Staff will utilize the electronic web-form, located on the CSPD Intranet, to log their criminal history check.

The commander of each investigative unit may appoint a limited number of office specialists and CSR/CSO to be responsible for performing criminal history checks and maintaining these records at their respective investigative unit. The Intelligence Unit may perform its own checks and maintain its own log sheet. That log sheet and a properly stamped copy of each Criminal History obtained will be placed in a sealed envelope and given to the clerk for submission, at the same time.

All other personnel of the department, when requesting criminal history checks, will go through the NCIC operator in the Records Section.

.26 Message Sending

The only terminal authorized to send NCIC and CCIC messages is the COJ terminal, NCIC Operator, in the Records Section. Any person wanting to send a message must have it approved by a supervisor. All messages will be recorded and maintained on file, as required by NCIC policy and State Archives laws.

.27 Operator Security Number

Supervisors may submit a request form to the department's CBI Coordinator to obtain an OSN, Operator Security Number, for sworn or civilian employees. Upon obtaining the OSN, the employee must complete the online computer test and complete a certificate of understanding, to be forwarded to the CBI Coordinator. In addition, the individual must also successfully complete the FBI's CJIS Security Awareness Training. This training will be coordinated by the CBI Coordinator or their designee.

Personnel who use department computers/MDC to access law enforcement/criminal justice records or systems will maintain an OSN via compliance with current state law and regulations governing OSNs. Questions regarding OSNs will be directed to the department's CBI Coordinator.

.28 NCIC/CCIC Queries

Employees with an OSN are encouraged to use the query screens to check offenders or possible offenders, vehicles, guns, etc., for "entries of interest." Queries can be made through the CAD system, the RMS system, or Open Fox. If a warrant confirmation is needed, the NCIC Operator must be contacted (444-7776) for assistance and proper documentation.

.29 Retention of Department Records

In order to maintain legal control of official reports and other official documents, the department maintains the official copy of all case reports and accident reports in the Records Section. The Record Section maintains these records in strict accordance with State and Federal law dealing with Criminal Justice Records, various court orders and rulings (such as orders sealing files, expungements, etc.), and various privacy laws designed to prevent identity theft.

It is imperative that unregulated duplicate copies of official files not exist and potentially circulate outside of the Records Section because of these legal requirements. This includes digital copies of documents as well as paper copies.

.30 Records Storage

Digital

All case information and digital evidence must be stored exclusively in an authorized location.

Current authorized locations are:

- LERMS / MFR
- Evidence.com
- CSPD Intelligence Systems

Unauthorized storage locations are, but not limited to:

- Group/Unit Share Drives (IE Patrol Drive, Library Drive, etc.)
- Personal file storage locations (IE Microsoft One Drive, Google Drive, etc.)
- Unapproved software applications
- Flash drives
- External hard drives / CDs / DVDs
- Personal computers, tablets, phones, or laptops

The only exception to deletion is if the data is stored on a physical medium that will immediately be placed into physical evidence. (IE flash drive, hard drive, CD, etc.)

The Records Section is authorized to store specified digital records on a "restricted access" Group Share drive to ensure compliance with record retention requirements as required by the Colorado Municipal Records Retention Schedule.

Physical

It is the position of CSPD that paper records will be converted to digital formats, when possible, to ensure proper security and storage in an authorized system.

Consideration should be given to the possible preservation of paper records that may be of a historical nature. Any records believed to have historical significance should be forwarded to the Division Commander for review by the CSPD Historical Committee.

Authorized locations for physical/paper records and PII include:

- The Record Section
- The Crime Analysis/Intelligence Unit
- The Evidence Unit
- Off-site archival storage (Iron Mountain, American Records, DocuVault, etc.)

From time-to-time members may retain "working copies" of paper reports to carry out their official duties. This includes such things as "working files" maintained by various investigators conducting follow-up inquiries, members retaining copies of reports until they are sure the report has been entered into the LERMS system, and members obtaining copies of files for court. These practices are permissible, provided certain practical safeguards are followed. It is the responsibility of personnel using the records to ensure proper storage and security.

Individual officers may retain physical copies of files only for three purposes:

- Assuring that the official copy of the file has been received and processed by the Records Section.
- Follow up investigations.
- For use in court after a subpoena or other official notice to appear has been received.

Once the permissible need no longer applies, the physical copies must be placed in a secured shred bin for destruction to prevent loss or misuse.

.32 Access to Department Records

Employees are granted access to department records systems solely to aid them in carrying out their assigned duties.

Employees who wish access to a record for non-department purposes must utilize the same procedures as any other member of the public. A schedule of fees for certain records has been established by various laws and regulations and is posted on the department's public-facing internet site.

.35 Modification of Records

To protect the integrity of official records and reduce potential liability, all additions, changes or deletions to official department records or automated records systems will be the responsibility of Records Section personnel as authorized by the Office of the Chief of Police, the Records Manager, and in consultation with the City Attorney's Office, if applicable.

.40 Security Clearances

Personnel who will view, process, or use departmental records or have access to automated criminal history records terminals will be record-checked before employment. The record check will consist of fingerprint clearances through the Colorado Bureau of Investigation (CBI); the Federal Bureau of Investigation (FBI); local criminal history check; local, state and federal warrant checks; Colorado Department of Revenue (DOR) checks; an extensive background check; and will include a polygraph examination. These procedures are in accordance with rules established in the

FBI CJIS Security Policy Manual and are necessary to ensure the security and confidentiality of departmental and automated records systems.

.50 Training

Department personnel responsible for adding, correcting, deleting, or disseminating departmental or automated systems records will attend training sessions on the proper use and control of such records. The Records Section Manager is responsible for ensuring that such training occurs.