Records Maintenance and Release

804.1 PURPOSE AND SCOPE

This policy provides guidance on the maintenance, access and release of department records. Protected information is separately covered in the Protected Information Policy.

804.2 POLICY

The Colorado State University Police Department is committed to providing public access to records in a manner that is consistent with the Colorado Criminal Justice Records Act (CCJRA) (CRS § 24-72-301 et seq.).

804.3 CUSTODIAN OF RECORDS RESPONSIBILITIES

The Chief of Police shall designate a Custodian of Records. The responsibilities of the Custodian of Records include but are not limited to (CRS § 24-72-301 et seq.):

(a) Managing the records management system for the Department, including the retention, archiving, release, and destruction of department records.

(b) Maintaining and updating the department records retention schedule including:

1. Identifying the minimum length of time the Department must keep records.
2. Identifying the department division responsible for the original record.

(c) Establishing rules regarding the inspection and copying of department records as reasonably necessary for the protection of such records.

(d) Identifying records or portions of records that are confidential under state or federal law and not open for inspection or copying.

(e) Establishing rules regarding the processing of subpoenas for the production of records.

(f) Ensuring the availability of a current schedule of fees for public records as allowed by law (CRS § 24-72-306).

804.4 PROCESSING REQUESTS FOR RECORDS

Any department member who receives a request for any record shall route the request to the Custodian of Records or the authorized designee.

804.4.1 REQUESTS FOR RECORDS

The processing of requests for any record is subject to the following:

(a) The Department is not required to create records that do not exist.

(b) When a record contains material with release restrictions and material that is not subject to release restrictions, the restricted material shall be redacted and the unrestricted material released.

1. A copy of the redacted release should be maintained in the case file for proof of what was actually released and as a place to document the reasons for the redactions. If the record is audio or video, a copy of the redacted audio/video release should be maintained in the department-approved media storage system and a notation should be made in the case file to document the release and the reasons for the redacted portions.

(c) The payment of any authorized fees required for the copying or mailing of the records requested as authorized by CRS § 24-72-306.

(d) Records related to arrests (i.e., official action) shall, and all other records may, be made available for inspection at reasonable times except as otherwise provided by law (CRS § 24-72-303; CRS § 24-72-304).

1. The Custodian of Records shall deny access to a requester seeking access to records unless the requester signs a statement which affirms that the records shall not be used for the direct solicitation of business for pecuniary gain (CRS § 24-72-305.5).

(e) If the records requested are related to an arrest and are in active use, in storage, or otherwise not readily available, the Custodian of Records shall notify the requester of the status. This notice shall be in writing if requested by the requester. If requested, the Custodian of Records shall set a date and hour, within three working days, at which the records will be available to the requester (CRS § 24-72-303):

1. If the Department does not have the records related to an arrest, the Custodian of Records shall include in the notice, in detail to the best of his/her knowledge and belief, the agency which has custody or control of the requested record.

(f) For all other records requested (i.e., not related to an arrest) that are not in the custody or control of the Department, the Custodian of Records shall notify the requester of the status. The notice shall be in writing if requested by the requester. The notice shall include the reason for the absence of the records from the Department's custody or control, their location, and what person has custody or control of the records (CRS § 24-72-304).

1. If the Custodian of Records has knowledge that the records requested are in the custody and control of the central repository for criminal justice records, the request shall be forwarded to the central repository.

(g) If the Custodian of Records denies access to a record and the applicant has requested a written statement of the grounds for the denial, the Custodian of Records shall prepare the written statement and provide it to the applicant within 72 hours, citing to the law or regulation under which access is denied or the general nature of the interest to be protected by the denial (CRS § 24-72-305).

(h) Records related to completed internal investigations (including any appeals) into the alleged misconduct of an in-uniform or on-duty officer, when involving a member of the public, shall be made available for inspection as required by CRS § 24-72-303.

804.5 RELEASE RESTRICTIONS

Examples of release restrictions include but are not limited to:

(a) Personal identifying information, including an individual's photograph; Social Security and driver identification numbers; name, address, and telephone number; and medical or disability information that is contained in any driver's license record, motor vehicle record or any department record, including traffic accident reports, are restricted except as authorized by the Department, and only when such use or disclosure is permitted or required by law to carry out a legitimate law enforcement purpose (18 USC § 2721; 18 USC § 2722).

(b) Victim information that may be protected by statutes (CRS § 24-4.1-303; CRS § 24-72-304).

(c) Juvenile-related information that may be protected by statutes (CRS § 19-1-304).

(d) Certain types of reports involving, but not limited to, child abuse or neglect (CRS § 19-1-307) and at-risk adult abuse (CRS § 26-3.1-102).

(e) Records that contain the notation "CHILD VICTIM" or "SEXUAL ASSAULT" shall have identifying information deleted as required by CRS § 24-72-304.

(f) Records that contain information concerning an application for victim's compensation (CRS § 24-4.1-107.5).

(g) Information received, made, or kept by the Safe2Tell® program (CRS § 24-31-607).

(h) Records of the investigations conducted by the Department, records of the intelligence information or security procedures of the Department, or any investigatory files compiled for any other law enforcement purpose (CRS § 24-72-305).

(i) The result of chemical biological substance testing (CRS § 24-72-305).

(j) The address of an individual who has requested and been approved for address confidentiality (CRS § 24-30-2108).

(k) Personnel records, medical records, and similar records which would involve personal privacy.

(l) Any other record subject to inspection where such inspection would be or is (CRS § 24-72-305):

1. Contrary to any state statute.
2. Prohibited by rules promulgated by the state supreme court or by order of any court.

804.6 SUBPOENAS AND DISCOVERY REQUESTS

Any member who receives a subpoena duces tecum or discovery request for records should promptly contact a supervisor and the Custodian of Records for review and processing. While a subpoena duces tecum may ultimately be subject to compliance, it is not an order from the court that will automatically require the release of the requested information.

Generally, discovery requests and subpoenas from criminal defendants and their authorized representatives (including attorneys) should be referred to the District Attorney, Office of General Counsel or the courts.

All questions regarding compliance with any subpoena duces tecum or discovery request should be promptly referred to legal counsel for the Department so that a timely response can be prepared.

804.7 RELEASED RECORDS TO BE MARKED

Each page of any written record released pursuant to this policy should be stamped in a colored ink or otherwise marked to indicate the department name and to whom the record was released. Released records shall be tracked and logged by Records Personnel.

Each audio/video recording released should include the department name and to whom the record was released.

804.8 EXPUNGEMENT OR SEALED RECORDS

Expungement orders or orders to seal criminal records received by the Department shall be reviewed for appropriate action by the Custodian of Records. The Custodian of Records shall expunge or seal such records as ordered by the court. Records may include but are not limited to a record of arrest, investigation, detention, or conviction. Once the record is expunged or sealed, members shall respond to any inquiry as though the record did not exist (CRS § 24-72-702; CRS § 24-72-703).

804.8.1 EXPUNGEMENT OF ARREST RECORDS RESULTING FROM MISTAKEN IDENTITY

If the Investigations supervisor determines that a person was arrested based on mistaken identity and no charges were filed following the arrest, the Custodian of Records shall file a petition for an order to expunge any arrest or criminal records resulting from the mistaken identity. The petition must be filed no later than 90 days after the investigation determines the mistaken identity, in the judicial district where the arrest occurred (CRS § 24-72-702).

804.8.2 EXPUNGEMENT OF CERTAIN JUVENILE RECORDS WITHOUT COURT ORDER

The Custodian of Records shall acknowledge receipt of a notice issued by the district attorney or other diversion provider that a juvenile has successfully completed a prefiling diversion. Upon receipt of the notice, the Custodian of Records shall treat the records as expunged within 35 days and without need of a court order (CRS § 19-1-306).

804.9 SECURITY BREACHES

Members who become aware that any Colorado State University Police Department system containing personal information may have been breached should notify the Custodian of Records as soon as practicable.

The Custodian of Records shall ensure the required notice is given to any resident of this state whose unsecured personal information is reasonably believed to have been acquired by an unauthorized person. If the security breach is reasonably believed to affect 500 or more Colorado residents, the Custodian of Records shall also notify the Colorado attorney general. Notice may not be required if the Custodian of Records, after a reasonable investigation, makes a determination

that misuse of the individual's information has not occurred and is not reasonably likely to occur. Additional notices to consumer reporting agencies may be required if the security breach requires notification to more than 1,000 Colorado residents (CRS § 24-73-103).

Notice shall be given in the most expedient time possible and without unreasonable delay, and not later than 30 days from the discovery of the breach, consistent with the needs of the department and any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system. Notice may be delayed if notification will impede a criminal investigation. In such cases, notice shall be made not later than 30 days after a determination is made that notification will no longer impede the investigation (CRS § 24-73-103).

For the purposes of the notice requirement, personal information includes an individual's first name or first initial and last name in combination with any one or more of the following when not encrypted, redacted, or secured by any other method that renders the information unreadable or unusable (CRS § 24-73-103):

(a) Social Security number

(b) Driver's license number or identification card number

(c) Student, military, passport, or health insurance identification number

(d) Medical information

(e) Biometric data

(f) Username or email address, in combination with a password or security questions and answers, that would permit access to an online account

(g) Full account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to the individual's account

If the breach reasonably appears to have been made to protected information covered in the Protected Information Policy, the Custodian of Records should promptly notify the appropriate member designated to oversee the security of protected information (see the Protected Information Policy).