

FREMONT CENTERVILLE LITTLE LEAUGE

ADMINISTRATIVE POLICY

SUBJECT: Criminal Offender Record Information – Management and Use Policy #: 001__

EFFECTIVE DATE: 03/01/2026

Purpose

FREMONT CENTERVILLE provides employees and officials with various tools and resources that enable them to perform their regular duties and assignments. This document defines policies, practices, and procedures for the access, retention, security, and destruction of both state and federal criminal offender record information (CORI) obtained from fingerprint-based background checks.

Background

FREMONT CENTERVILLE wants to ensure the security and confidentiality of criminal offender record information (CORI) in accordance with the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Policy and pertinent California Department of Justice policies.

Scope

This policy applies to the Custodian of Records (COR), employees, officials, and/or hiring authorities charged with determining the suitability of an applicant for employment, licensing, volunteer, and/or certification.

Policy Statements

It is the policy of **FREMONT CENTERVILLE** that:

1. Personally owned information systems shall not be authorized to access, process, store, or transmit CORI unless the need is determined and specific terms and conditions for personally owned information system usage have been established (Ref. [CJIS Security Policy](#))
2. Publicly accessible computers shall not be used to access, process, store or transmit CORI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc. (Ref. [CJIS Security Policy](#)).
3. The COR will shred/destroy the CORI in physical form and/or electronic media obtained for employment, licensing, volunteer, and/or certification once a decision is made to employ, license, or certify the subject of the record.

"Electronic media" is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" refers to CORI in physical form, e.g. printed documents.

(If applicable to your agency:) Retention beyond this time will be based on a legitimate business need approved in writing by the Agency Head. As such:

- 3.1 CORI will be stored in a physically secure and confidential location (e.g., a locked area, room, or file cabinet), with both physical and personnel security controls preventing unauthorized access and viewing. CORI kept in an electronic format will also be protected at the same level as physical media.
- 3.2 CORI transported outside the secure location must be carried in a locked container and will be protected in transit.
- 3.3 CORI will not be sent via email unless the proper technical controls are in place to protect it, such as encryption and access control (i.e., password). Email is not a secure method of transmitting CORI without these control measures.
- 3.4 The COR will shed/destroy the physical media and/or electronic media when no longer required.

FREMONT CENTERVILLE LITTLE LEAGUE

ADMINISTRATIVE POLICY

SUBJECT: Criminal Offender Record Information – Management and Use Policy #: 001__

EFFECTIVE DATE: 03/01/2026

- 3.5 The COR will sanitize or destroy electronic media (electronically overwrite the data at least three times) or degauss electronic media before disposal or release for reuse.
4. The COR will immediately (within one hour of discovery) notify the DOJ of any security incident including unauthorized access to CORI. Information concerning the security incident will be recorded and reported by using the California Department of Justice's (DOJ) IT Incident Report Form (part of this document) for Noncriminal Justice Agencies.

Using the same Form, the COR, within five calendar days of such discovery, will provide the DOJ with a written report documenting the corrective action(s) taken to resolve the security incident.

Possible Consequences of CORI Mismanagement and/or Misuses:

Observance of these policies and procedures is essential to the delivery of agency services and programs and to the integrity, security, and confidentiality of CORI. Violation of these or other policies or information systems may constitute a failure to perform regular duties and assignments, and may result in any or all of the following:

- Reporting of the incident(s) to management;
- Possible revocation of access privileges;
- Possible disciplinary action in accordance with Civil Service Rules, up to and including termination.
- Unauthorized access, disclosure, and/or misuse of CORI is a criminal offense. (Penal Code §§ 11140 through 11144 (prescribing the penalties for misuse of criminal history record information); Government Code §§ 6200, 6201 (prescribing the penalties for the misuse of various government records, which include criminal history record information)).

Approved:



Nanette Hamilton
CORI - Agency Head

FREMONT CENTERVILLE LITTLE LEAGUE

ADMINISTRATIVE POLICY

SUBJECT: Criminal Offender Record Information – Management and Use Policy #: 001_

EFFECTIVE DATE: 03/01/2026

**IT Incident Report Form for Noncriminal Justice Agency
Department of Justice
Authorization and Certification Program**

| Contact Information for this Incident | |
|--|-------------------|
| Agency Name: | |
| Phone Number: | Date of Report: |
| Person Reporting Incident: | |
| Incident Description | |
| Date of the Incident: | Point of Contact: |
| Location(s) of Incident: | |
| Systems Affected: | |
| Method of detection: | |
| Who detected it: | |
| Nature of Incident | |
| <input type="checkbox"/> Security Incident: | |
| <input type="checkbox"/> Security Breach: | |
| Provide a brief description: | |

FREMONT CENTERVILLE LITTLE LEAGUE

ADMINISTRATIVE POLICY

SUBJECT: Criminal Offender Record Information – Management and Use Policy #: 001__

EFFECTIVE DATE: 03/01/2026

| Sensitivity of Data/Information Involved |
|--|
| Type of Information Accessed: |
| Total duration of Incident: |
| Actions Taken/Resolution: |
| What is being done to prevent it from repeating? |
| Please elaborate: |

Please submit the incident report to:
Shelley Rider, Staff Services Manager
Training and Administrative Support Section
Authorization and Certification Program in the Department of Justice
Shelley.rider@doj.ca.gov