



Effective: 04/02/1999
Last Revised: 09/15/2019

**CSU FULLERTON POLICE DEPARTMENT
GENERAL ORDER NUMBER 7-6**

RECORDS UNIT

- SUBJECT:** Management of all Department generated Law Enforcement, operational, and information records and files.
- PURPOSE:** The below operating policy and procedures are to ensure adherence to the California Department of Justice (DOJ) and California Public Records-*Government Code Section 6250-6265* regulations regarding the protection, storage, and maintenance of University Police Department records and files.
- POLICY:** CSU Fullerton Police Department uses an electronic Records Management System (RIMS) that links the Communications Center dispatching, law enforcement field reporting, police records, evidence, found/agency-owned property control, and investigative case management. The Department's Records Unit responsibilities include the processing, scanning and entry of all police reports, reporting statistical information to the State and Federal Government, court arrest processing, and releasing of records under the regulations of the law as required by law.

PROCEDURE:

- I. Confidentiality and Security of Records [CALEA 82.1.1a]
- A. DOJ regulations require that Police Records be restricted to personnel who have had background checks and fingerprint clearances from the DOJ and the FBI. Access to records is limited to:
1. Records Supervisor, Communications Supervisor, dispatchers, watch commanders and records clerks.
 2. The Chief of Police and Command Staff.
 3. Police Officers on necessary official business.
 4. Community Service Officers (CSO's) or student assistants assigned to the Records Unit.
 5. Other Department employees when on official business.
 6. Equipment service technicians and custodians may only enter this area while directly supervised by authorized Department personnel.

- B. Every University Police Department employee will sign an agreement that ensures the confidentiality of all Department records and files. Security of the records and the integrity of the system are enhanced by utilizing the following procedures.
1. The Records office is located off the main lobby in a locked room with security doors restricting entry to the Department offices to the following personnel:
 - a. All authorized Department employees who have the required key card.
 - b. Persons admitted by Dispatch who control entry electronically.
 2. The Records Office is clearly posted "Authorized Personnel Only." The following records are available by computer query to authorized personnel 24-hours a day [CALEA 82.1.7, 82.1.1b]:
 - a. Case Reports from 1996 are accessed in RIMS and the original hard copies of the current year and the previous six years are maintained in the Master Case Reports File.
 - b. Criminal history inquiries are accessed through the California Law Enforcement Telecommunications System (CLETS) terminal.
 - c. National Crime Information Center (NCIC) reports (DMV, stolen vehicles and property, missing persons) are accessed through the CLETS terminal.
 - d. Daily logs of all incidents from the Computer Aided Dispatch (CAD) program and pertinent Active Restraining Orders.
 - e. Found Lost Property/Safekeeping are also cataloged and stored in the Records Office.

II. Department Record-keeping and Retention

- A. All reports/records/files will be retained and destroyed consistent with State of California legal requirements, see the CSU Fullerton Police Department Records Retention Schedule. [CALEA 82.1.3]
- B. The original of all University Police case reports will be maintained in numerical order in the Master Case Reports files.
- C. Under no circumstances will the original report be removed from the Records Unit, only copies will be routed to the appropriate personnel for follow-up as required. [CALEA 82.2.4, 82.3.5, 82.1.5]
1. Arrest, crime, traffic, complaint, and incident reports prior to the immediate past year are locked in the records archives. The Records Supervisor and the designated Records Technician and Records Community Service Officers maintain the keys for entry.
 2. Personnel Files, Background Investigation Files, and Personnel Complaint Files on current employees are secured in the Chief's Office and files on past employees are stored in Administration Storage under the direct

3. The Investigators retain copies of all cases actively under investigation and those cases used for crime prevention training.
 4. Reports on damage to campus property, personal injury, and/or any possible liability claims against the Department, University, and/or the State of California will be handled as outlined in General Order 7-9.
 5. Patrol operations and special events records, along with all "Use of Force" and "Pursuits" case copies are maintained in the office of the appropriate Command Staff.
 6. The Community Services Corporal maintains Community Service Officer and program records and community outreach crime prevention records.
 7. Payroll-attendance files, Department budgets/records, and all fiscal records are securely maintained and stored in accordance with the retention schedule in a locked office by the Department's Budget Manager.
 8. Both the Support Services Unit and University Auto Shop maintain the Department owned fleet records.
 9. The Police Records Supervisor maintains the records on property and items for safekeeping.
 10. The Property and Evidence Custodian maintains all the evidence records.
 11. Warrants/wanted person and communications records are under the custodial care of the Records Supervisor.
 12. All workstation records are securely maintained and access to various security levels in each program is authorized by an individual's name and password.
 13. The Records Supervisor maintains the master set of keys for all records/files. Lock changes will be made when the custodian changes or by order of the Chief to ensure security.
 14. It is the responsibility of all designated custodians to ensure that access to the confidential files is handled on a need to know basis. The Chief of Police will resolve conflicts relating to the legitimate need to access confidential files.
- D. Prior to submission to the Records Unit for further data entry and storage, each police report will be reviewed by the Watch Commander for completeness. The appropriate Watch Commander will approve the report and forward it to the Records Unit (Refer to General Order 5-2).

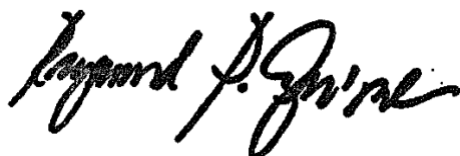
- E. All the originals are filed in the Master Case Reports file in the Records archives after they have been completed and approved in RIMS. [CALEA 82.1.5]
1. The Investigative Sergeant will screen the case reports and determine what type of follow-up is required and route the case to the appropriate individual or department.
 2. All follow-up reports should be prepared within ten days from date of assignment.
 3. As follow-up reports, supplements and status reports are received by the Records Unit, the case number is crosschecked and verified. Then these documents will be filed with the original report.
- F. The Records Supervisor will be responsible handling, transporting, storing and destroying all media containing CLETS information by shredding or burning, to the point that any reconstruction of the record is impossible.
- G. The Records Supervisor will be responsible and accountable for the collection, maintenance, dissemination, retention, and destruction of juvenile records.
1. All juvenile arrest and identification records will be collected, retained, disseminated, and destroyed in strict compliance with existing statutes, decisional law, and policies or orders by the Juvenile Court for the County of Orange.
 2. Juveniles will not be fingerprinted and photographed unless the Officer determines that fingerprinting and photographing of the juvenile offender is necessary (e.g. serious offenses and felonies). [CALEA 82.1.2b]
 3. All juvenile arrest and/or identification records (fingerprints, photographs or physical descriptions) will be affixed to the original report and clearly marked **JUVENILE** prior to copying or filing. [CALEA 82.1.2a,b]
 4. These records will include a clear designation and protection in the Case Management and Master Name File programs of the Records Management System (RIMS). [CALEA 82.1.2a,c]
 5. All juvenile records will be filed in a separate locked file cabinet, retained until reaching the age required for purging designating the case as a juvenile record will be placed in the Master Case Reports file. [CALEA 82.1.2a,c,d]
 6. Access to juvenile records will be limited to those with both “a right and a need to know.” This will be in strict compliance with all existing State and Federal Laws. [CALEA 82.1.2c]
 7. Upon receipt of a Court Order to seal or expunge an official police record, the Records Unit Supervisor will be responsible for ensuring the prompt sealing or shredding of the indicated record(s). [CALEA 82.1.2e]
- H. The Department’s case records and arrest details are confidential and not open to inspection by the general public (California Information Practice Act). Records personnel will comply with the following procedures [CALEA 82.1.1c]:
1. All requests from individuals outside law enforcement must be submitted in

- writing and the Records Supervisor must approve the release of copies.
2. Traffic accident reports or a copy of an individual's statements will only be released to person(s) involved or their representative.
 3. The authorized request form will be attached to the original case report.
- I. On a monthly basis, the Records Supervisor will compile and submit Uniform Crime Report (UCR) statistics to the California Department of Justice (DOJ). These statistics will be collected according to Federal Bureau of Investigation (FBI) guidelines. [CALEA 82.1.4]
- J. The main server for RIMS and the RIMS application has four levels of security. The server is behind a firewall that allows only the designated computer IP addresses identified by the Police Department access. Each computer has a pre-selected security level for the RIMS program. Only Department personnel with the appropriate network ID and password can access these computers. The Communications and Records Unit will ensure the protection of the computerized records/reports/files with the following measures [CALEA 82.1.6c]:
1. All RIMS computer files are backed up daily and are sent weekly to an off-site secure location. [CALEA 82.1.6a,b]
 2. The Department will ensure that all programs used are properly licensed. Employees will not introduce any non-authorized software or disks into the computer system or Department laptops or workstations. All computers will continually scan any disk or download for viruses [CALEA 11.4.4].
 3. The integrity of the records computer system is maintained in two ways. The computers have a configured functional use security level for the RIMS program. The RIMS application requires personnel to be identified as a user with a unique ID, password and security level. The security levels allow limited or unlimited access to the program. [CALEA 82.1.6d]
 4. Administration and Finance Division IT will provide a systems analyst who will perform annual audits of the Records Unit computer systems to verify all passwords, access codes are authorized. They will check the systems for any apparent access violations. [CALEA 82.1.6d]

REVIEWED BY:

G. Dack

APPROVED:



Raymund Aguirre
Chief of Police