CRIMINAL HISTORY INFORMATION

GENERAL ORDER #16.00

Adopted: 6/01/05	**Pages:** 5
Persons Affected: All Sworn	**Authority:** Laura Wilson, Director
IACLEA Standards: 16.1.9	

Revision History

Replaces SUDPS General Order #3.1.7(06/01/05)
Updated: 01/25/2023

POLICY

Sworn members of the Stanford University Department of Public Safety shall obtain and use criminal history only for official business of the Sheriff's Office. Any employee who violates this policy will be subject to disciplinary action and may be subject to criminal prosecution.

PROCEDURE

A. USE OF CLETS

1. The California Department of Justice is responsible for the California Law Enforcement Telecommunications System (CLETS). This computerized system provides criminal history information and communications with state, federal and international law enforcement agencies.

2. Information accessed through CLETS is strictly confidential and is to be used for law enforcement purposes only.

3. The use of the CLETS system is governed by the provisions of the CLETS User's Agreement. The Department Agency Terminal Coordinator (ATC) is to ensure that all CLETS access equipment is installed and maintained as required by the CLETS agreement.

4. The use of the CLETS system also is governed by applicable provisions of criminal law, including Penal Code sections 182, 502, 11140-11143, and 13300 -13304, and Vehicle Code section 1808.45. The use of CLETS for other than authorized law enforcement purposes can be prosecuted criminally if the conduct violates the provisions of the criminal law.

5. *Sworn members of the Stanford University Department of Public Safety* shall use the CLETS system in compliance with applicable law and agreements. *Sworn members of the Stanford University Department of Public Safety* shall obtain and use information from the CLETS system for official business of the *Department*.

B. CORI – CRIMINAL OFFENDER RECORD INFORMATION

1. Criminal Offender Record Information (CORI), also known as Criminal History Record Information (CHRI), is not public information, and is subject to the provisions of sections 11075-11081 and 13300 - 13304 of the California Penal Code. This information includes arrest summaries, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release.

2. Criminal Offender Record Information is maintained at the *Stanford University Department of Public Safety* in various forms. It includes information maintained in the CLETS system as well as information contained in Santa Clara County's Criminal Justice Information Control (CJIC) system and hard copy files.

C. CRIMINAL JUSTICE INFORMATION

1. Criminal Justice Information (CJI) is any information collected, stored, maintained, or obtained from a criminal justice database, such as information obtained from CLETS and CJIC. CJI is sensitive information and should be safeguarded to prevent unauthorized or improper access, use or dissemination and release.

2. Criminal Justice Information Services (CJIS) includes any system used to process, store, or transmit CJI.

D. SECURITY OF CRIMINAL JUSTICE INFORMATION

1. Access to criminal offender record information is restricted by law to those who have both the right to know and the need to know. Employees with access to criminal

offender record information shall comply with all applicable law and agreements regarding confidentiality of the information obtained. *Sworn members of the Stanford University Department of Public Safety* shall obtain and use criminal offender record information *only* for official business of the *Department*. *Sworn members of the Stanford University Department of Public Safety* shall document the use and disclosure of all criminal history information as provided in the applicable law and agreements regarding confidentiality of the information obtained.

2. Only personnel specifically designated by the *Director of Public Safety* are authorized to release or photocopy criminal offender record information. No other personnel shall release criminal offender record information except as specifically authorized in a direct or written order and then only to persons who are authorized to receive such information.

3. The District Attorney's Office will be provided with criminal offender record information at the time that criminal charges are requested based on a criminal investigation conducted by the Sheriff's Office.

4. *Sworn members of the Stanford University Department of Public Safety* authorized to release or photocopy criminal offender record information shall determine whether the person receiving the information has a right to know and a need to know, except when the release of information is pursuant to a court order or other legal process. The fact that the person making the request is a peace officer does not relieve the employee of his or her responsibility to maintain the confidentiality of the information.

5. No employee shall destroy criminal offender record information except in compliance with the procedures specified in the CLETS User's Agreement and the applicable provisions of law.

6. *Sworn members of the Stanford University Department of Public Safety* authorized to access CLETS, CORI or Confidential databases are issued individual user identifications and confidential passwords. Staff will not give out or share their user identifications or confidential passwords, use another person's user identification or confidential passwords, or allow their user identifications or confidential passwords to be used by another person.

7. CLETS and CORI access terminals/computers will be located in a secure area, accessible only to authorized staff and never in the view of the public or inmates. Terminal/computer screens shall use a privacy screen protector when necessary and monitors will be cleared and computers locked when not in use to ensure that confidential information is not displayed unnecessarily.

8. The processing and storing of CJI shall remain in secure areas. Doors will remain

locked to prevent unauthorized access. Visitors must be escorted by authorized personnel at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein.

9. Staff will exercise caution to ensure that unauthorized persons do not have access to transmitted confidential documents. Voice-to-voice contact and authorized receiver verification should occur before, or at the time of, CORI transmissions. Voice transmission of CJI should be limited and details of a criminal history should only be given over a radio or cell phone when an officer determines there is an immediate need for the CJI to further an investigation or situations affecting the safety of an officer or the general public. Fax machines that receive CORI shall be in a secure area. Confidential information will only be faxed in extenuating circumstances. Before transmitting any confidential document, staff must verify the receiving agency is authorized to receive the information, verify the correct fax number, avoid misdialing and confirm the receiving fax is in a secured location.

E. DESTRUCTION OF CRIMINAL JUSTICE INFORMATION

1. CORI, Criminal History and Criminal Justice Information must only be used for its intended authorized purpose for which it was requested and then it must be destroyed.

2. When ready for destruction, hard copy files and electronic media must be placed in a locked security bin. The contents in the security bins will be shred once a week by an onsite shredding company that is escorted throughout the building as well as during the shredding process.

F. REPORTING MISUSE OR SECURITY INCIDENTS

1. All *Sworn members of the Stanford University Department of Public Safety* are responsible for reporting suspected misuse of CLETS, CORI, Confidential information or a suspected security incident.

2. To report the suspected misuse of information:

   A. Employees must submit an Administrative Report to their immediate supervisor describing the circumstances. If their immediate supervisor is unavailable, the employee will notify the next person in the chain of command or the on-duty Watch Commander.

   B. It shall be the responsibility of the immediate supervisor to promptly notify their superior in the chain of command.

C. Notification will be made to the Investigations Division and Internal Affairs Unit.

D. The Investigation Division and Internal Affairs Unit will investigate accordingly.

3. To report a suspected security incident or a breach of CJI:

A. Employees must provide the following information to the Information Security Officer (ISO) or their designated representative(s).

1. Date of incident, location of incident, systems affected, method of detection, nature of incident, actions taken/resolution, date and contact info for agency.

G. MISUSE OF CRIMINAL JUSTICE INFORMATION

1. Any employee, volunteer, or intern of the *Stanford University Department of Public Safety* who misuses Criminal Justice information may result in any one or combination of the following actions:

A. Disciplinary action

B. Dismissal from employment

C. Criminal prosecution

D. Civil liability