Sacramento County **Probation Department**

GENERAL ORDER

Access to Automated Record Systems

Purpose and Scope

This order provides standards governing the access and security of information and/or data collected, stored, or accessible to employees of the Sacramento County Probation Department and subject to any access or use restrictions imposed by law, regulation, order, or use agreement.

Rules governing the disclosure of information can be found in the *Disclosure of Records, Reports and Information General Order.*

Affected Personnel

All employees, contractors, interns and volunteers

Effective Date

Upon execution by the Chief Probation Officer

I. Standards

A. Employees shall not access, or attempt to access information that identifies a specific person, including an individual's photograph, social security number, driver's license number, name, address, telephone number, medical or disability information, or criminal record contained in any local, state or federal automated system, driver's license record, motor vehicle record, or any department record except as authorized and only when such access is permitted in accordance with their official duties or as required by law to carry out a legitimate law enforcement purpose.

B. Both a right to know and need to know must be present prior to accessing information obtained from any automated local, state or federal computer database, or department file. By statute and for lawful business needs, an individual may have the right to know specified information; however, the individual must also have a need to know the information for official, work-related purposes.

C. Unauthorized access to information contained in any automated local, state or federal computer application or system, or department file other than for legitimate work-related purpose is prohibited and may subject an employee to administrative sanction, civil action and/or criminal prosecution.

D. The following are examples of prohibited/unauthorized use of a specific system, e.g. CLETS, by federal, state or local law enforcement agencies:

1. Inquiring of yourself, a family member, friend, etc.;
2. Providing information from the CLETS to another officer, individual, agency or company for unauthorized purposes;
3. Sharing user ID's or passwords;
4. Logging into the CLETS and allowing others to utilize your authorized access;
5. Inquiring the Automated Criminal History System for licensing, employment or certification purposes (e.g., Carry Concealed Weapon permits);
6. Inquiring if a firearm, for your personal use, is stolen, prior to a purchase;
7. Inquiring to the DMV to obtain unauthorized address, vehicle registration, or insurance information (e.g., a vehicle parked in front of your house for two days);
8. Inquiring about high profile individuals in the media; and
9. Using any non-criminal history information contained within these databases for immigration enforcement purposes. This restriction does not pertain to information that is regarding a person's immigration or citizenship status pursuant to (8 U.S.C 1373 and 1644

E. Local, state and federal computer applications and systems include, but are not limited to:

1. Person Information Program (PIP)
2. Juvenile Probation Information Program (JPIP)
3. Criminal Justice Information System (CJIS)
4. California Law Enforcement Telecommunications System (CLETS)
5. Criminal History System (CHS)
6. National Crime Information Center (NCIC)
7. National Law Enforcement Telecommunications System (NCLETS)
8. Child Welfare Services/Case Management System (CWS/CMS)
9. LexisNexis/Accurint
10. Cal-photo: CA Department of Justice/Department of Motor Vehicles
11. Web Mug Shots
12. Known Persons Finder (WebKPF)
13. Sacramento County Sheriff's Department Report Management System (RMS)

F. Penal Code §§ 11140-11143 identifies individuals who are authorized access to information contained in automated records, and under what circumstances that information may be released. Information obtained shall only be disclosed to those persons having legal authority either by statute or court order.

G. Periodic driver license checks may be conducted on the CLETS subscribing agency employees where driving is a requirement of their job.

II. Information Security

A. Employees accessing or receiving restricted information shall ensure the information is not accessed or received by unauthorized persons.

B. Employees shall ensure automated systems and applications, and/or documents containing restricted information, are not accessible to others (e.g., on an unattended table or desk, in or on an unattended vehicle; on a computer terminal – attended or unattended).

C. Per the California Department of Justice, additional security, compliance requirements include:

1. Tilt or turn monitors, including those with privacy screens, away from doors and windows.
2. Place lids over all uncovered confidential paper bins.
3. Do not remove privacy screens from computers that may be visible to the public or clients.
4. Keep blinds at an angle which will prevent viewing of information contained on monitors through windows (this includes 2nd and 3rd floors).
5. Place printers in places not accessible to the public or clients.
6. Offices located in areas accessible to clients or the public are to be closed and locked when not occupied by Probation Employees.
7. Printed materials containing CORI (Criminal Offender Record Information) should be face down, in files or not on the desk when not being worked with.
8. Documents containing CORI data should only be shared with individuals meeting the need to know right to know criteria.

D. The Chief Probation Officer shall designate an employee to oversee the security of restricted information. The responsibilities include, but are not limited to:

1. Developing and maintaining security practices, procedures, and training;
2. Ensuring federal and state compliance with the Criminal Justice Information System (CJIS) Security Policy and the requirements of any state or local criminal history records system; and
3. Establishing procedures to provide for the preparation, prevention, detection, analysis and containment of security incidents. Documenting and reporting all security breaches to the Chief Probation Officer and appropriate authorities.

III. Training

All employees authorized to access and use restricted information shall complete training that complies with any restricted information system requirements and identifies authorized access and use of restricted information, as well as its proper handling and dissemination.

All employees authorized to access and use restricted information sign an acknowledgment form of this General Order which addresses the following: confidentiality, release and misuse of information, and employee discipline actions should misuse occur.

References

California Criminal Justice Information Security Policy
California Penal Code
California Government Code
California Vehicle Code
California Code of Regulations

Amends/Replaces

Amends Access to Automated Record Systems – February 2017

Authorized By _____ **Date** 10/31/19

Lee Seale, Chief Probation Officer