CLETS, SmartJustice and Protected Information

800.1 PURPOSE AND SCOPE

To set forth the policy and procedures with respect to access, transmission, release and security of protected information supplied by the California Law Enforcement Telecommunications System (CLETS), and the California SmartJustice system. This policy addresses the protected information covered in the day-to-day operation of the Riverside County Probation Department. This policy applies to all employees, contractors, volunteers and interns of the department.

800.1.1 DEFINITIONS

Definitions related to this policy include:

CLETS – California Law Enforcement Telecommunications System.

California SmartJustice – A database to facilitate the data sharing between counties, law enforcement, and public safety agencies to effectively supervise individuals, measure outcomes of re-entry programs and adult services, and properly manage resources.

CORI – Criminal Offender Record Information – As defined in Penal Code section 11075, “criminal offender record information” means records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release.

Protected Information – Any information or data that is collected, stored or accessed by the employees of the department and is subject to any access or release restrictions imposed by law, regulations, order or use agreement. This includes all information contained in federal, state and/or local law enforcement databases that is not accessible to the public.

Employees – This term refers to all employees: sworn and non-sworn, part-time and fulltime, contractors, volunteers and interns.

800.2 AUTHORITY AND REFERENCES

- Executive Committee;
- California Department of Justice;
- Federal Bureau of Investigation (FBI);
- Penal Code §§ 11143 & 13321;
- Title 11 of California Code of Regulations 702;
- California SmartJustice Policies, Practices, and Procedures (PPPs).

800.3 POLICY

Access/inquiry into the CLETS and SmartJustice systems by authorized operators and dissemination of information obtained are limited to the purpose(s) specified by law and federal,

state and local regulations. Employees will adhere to all applicable laws, orders, regulations, use agreements and training related to the access, use, dissemination and release of protected information.

800.4 RESPONSIBILITIES

The Chief Probation Officer shall select an employee of the department as the Agency CLETS Coordinator (ACC) to coordinate the use of protected information. The Chief Probation Officer shall also select a SmartJustice Agency Coordinator (AC) to review matters pertaining to the use of SmartJustice. Additionally, the Chief Probation Officer shall select a SmartJustice Security Point of Contact (SPOC) who will serve as the security coordinator pertaining to the use of SmartJustice. The responsibilities of these positions include, but are not limited to:

(a) Ensuring employee compliance with this policy and with requirements applicable to protected information, including requirements for the National Crime Information Center (NCIC) system, National Law Enforcement Telecommunications System (NLETS), Department of Motor Vehicle (DMV) records, SmartJustice and CLETS.

(b) Developing, disseminating and maintaining procedures that adopt or comply with the U.S. Department of Justice's current Criminal Justice Information Services (CJIS) security policy.

(c) Developing, disseminating and maintaining any other procedures necessary to comply with any other requirements for the access, use, dissemination, release and security of protected information.

(d) Developing procedures to ensure training and certification requirements are met.

(e) Resolving specific questions that arise regarding authorized recipients of protected information.

(f) Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

800.5 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, use agreement, the department's policies or training. Only those employees who have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the employee has a legitimate work-related reason for such access.

No employee shall access and query the CLETS and/or SmartJustice systems unless they have been duly authorized and designated, in writing, by the department as a CLETS and/or SmartJustice operator, and completed/fulfilled all necessary Department of Justice and the department's regulations.

Access/inquiry into the CLETS and SmartJustice systems by authorized operators is limited to the purpose(s) specified by law and Department of Justice regulations. With the exception of the Human Resources Division who shall operate within specified Department of Justice regulations,

no employee shall query the CLETS or SmartJustice systems to obtain information on themselves, an employee or any person outside the jurisdiction of the department.

Unauthorized access, including access for other than a legitimate work-related purpose, is prohibited and may subject the employee to administrative action and/or criminal prosecution.

Employees shall not inquire into their own record or have some other employee inquire for them.

Public access to an area where the CLETS-capable equipment is maintained is not authorized.

An appropriate log must be kept and filled out when any access/inquiry is made into the CLETS and when information received from same is disseminated to any person/agency outside the department. CLETS operators must make a corresponding entry in the Juvenile Adult Management System (JAMS) each time the CLETS is accessed. It is imperative the department justifies all the CLETS requests and the requests follow the “need to know” and “right to know” guidelines.

An appropriate log must be kept and filled out when any accidental access/inquiry is made into the SmartJustice system and when information received from same is disseminated to any person/ agency outside the department. SmartJustice operators; however, must make an entry in the JAMS each time the SmartJustice system is accessed. It is imperative the department justifies all the SmartJustice requests and the requests follow the “need to know” and “right to know” guidelines.

All logs and records pertaining to the access/inquiry of the CLETS/SmartJustice shall be maintained in accordance with DOJ and County of Riverside policies and procedures.

A designated CLETS/SmartJustice operator at each office shall be responsible for maintenance of telecommunication operating manuals and dissemination of updated information and regulations forwarded to them.

800.6 SMARTJUSTICE MISUSE

Violation of the California SmartJustice PPPs shall be investigated by the agency head or his/her designee and reported to the CalDOJ.

All SmartJustice subscribing agencies shall submit a report to the CalDOJ on the number of investigations performed related to the SmartJustice misuse, and any disciplinary action taken. This report will be submitted by February 1 of each year for the preceding calendar year even if no misuse was investigated. This information will be submitted on the SmartJustice Misuse Investigation Reporting sheet (attachment).

800.7 PENALTIES FOR MISUSE OF RECORDS

Giving/sharing the CLETS or SmartJustice operator code to any other person is prohibited.

It is a misdemeanor to furnish, buy, receive or possess Department of Justice criminal history information without authorization by law (Penal Code § 11143).

Authorized persons or agencies violating state regulations regarding the security of Criminal Offender Record Information (CORI) maintained by the California Department of Justice may lose direct access to CORI (11 CCR § 702).

Accessing and/or releasing information from SmartJustice for non-law enforcement purposes is prohibited and is subject to administrative action and/or criminal prosecution.

800.8 RELEASE OR DISSEMINATION OF PROTECTED INFORMATION

Protected information may be released only to authorized recipients who have both a right to know and a need to know.

Unless otherwise ordered or when an investigation would be jeopardized, protected information maintained by the department may generally be shared with authorized persons from other law enforcement agencies who have the right to know and the need to know and who are assisting in an investigation or conducting a related investigation. Any such information shall only be released after proper coordination with a supervisor.

Any request for the release of information provided by the CLETS/SmartJustice from an agency other than a CLETS subscribing agency shall be referred to the department's ACC. The department's ACC will verify the requestor's right and need to know and will prepare and submit to the Department of Justice the appropriate documentation (Release of Information from the California Law Enforcement Telecommunication System (CLETS) form) (attachment) as required by the Department of Justice and prior to the release of any such information. The release of said information is contingent upon the approval of the Department of Justice. Said form is to be filled out, signed and dated by the Chief Probation Officer and the department's ACC. The department's ACC shall retain a copy of the documentation in an appropriate file.

When requests for information are received from unknown parties over the telephone, identities shall be verified first by either calling the requesting agency directly to confirm and or by requiring a written request on appropriate letterhead. Written requests shall be confirmed by telephoning the agency. Once the person's identity has been verified, the person's right to know and need to know must be established.

Any person who requests the release of protected information without proper authorization shall be referred to a supervisor, the department's Custodian of Records and to the department's ACC.

Protected information, such as the Criminal Justice Information (CJI), which includes Criminal Offender Record Information (CORI), shall not be transmitted by radio, cellular telephone or any other type of wireless transmission to the employees in the field or in vehicles through any computer or electronic device, except in cases where there is an immediate need for the information to further an investigation or where circumstances reasonably indicate that the immediate safety of officers, other department employees or the public is at risk.

Nothing in this policy is intended to prohibit broadcasting warrant information.

800.9 REVIEW OF CRIMINAL OFFENDER RECORD

Individuals requesting to review their own California criminal history information shall be referred to the Department of Justice (Penal Code § 11121).

800.10 SECURITY OF PROTECTED INFORMATION

The Chief Probation Officer shall select an employee of the department (e.g. the IT Manager or designee) to oversee the security of protected information. The responsibilities of this position include, but are not limited to:

(a) Developing and maintaining security practices, procedures and training.

(b) Ensuring federal and state compliance with the CJIS security policy, SmartJustice PPPs, and the requirements of any state or local criminal history records systems.

(c) Establishing procedures to provide for the preparation, prevention, detection, analysis andcontainment of security incidents including computer attacks.

(d) Tracking, documenting and reporting all breach of security incidents to the Chief Probation Officer and appropriate authorities as outlined in the Riverside County Probation Department CLETS/SmartJustice Security Incident Response Plan (attachment).

800.11 EMPLOYEE RESPONSIBILITIES

Employees accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized to access or receive it. This includes leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (e.g. on an unattended table or desk; in or on an unattended vehicle, in an unlocked desk drawer or file cabinet; on an unattended computer terminal).

Any known violation of the above shall be reported immediately to a supervisor or the department's ACC, AC, and/or SPOC.

In case of a suspected or an actual breach of security of the CLETS or SmartJustice system, employees shall inform a supervisor and the department's ACC, AC and/or SPOC. The ACC, AC and/or SPOC shall notify the CalDOJ by electronic mail when a security incident is known and follow the guidelines outlined in the Riverside County Probation Department CLETS/SmartJustice Security Incident Response Plan (attachment). The SmartJustice incident shall also be reported to CalDOJ [redacted]

800.12 TRAINING

All employees authorized to access or release protected information shall complete the mandated Department of Justice and FBI training programs that comply with any protected information system requirement and identify authorized access and use of protected information, as well as its proper handling and dissemination.

CLETS, SmartJustice and Protected Information

Date(s) revised:

12/07/2017

06/13/2016

10/08/2010

05/12/2009

06/01/1992

Created: 11/09/1988

Attachments:

1. Riverside County Probation Department CLETS/SmartJustice Security Incident Response Plan

[redacted]

Riverside County Probation Department

CLETS/SmartJustice Security Incident Response Plan

A. Purpose

The CLETS/SmartJustice Security Incident Response Plan sets the guidelines for responding and/or reporting a CLETS/SmartJustice security incident at the Riverside County Probation Department. Examples of CLETS/SmartJustice security incidents are: stolen computer, virus/malware on computer, or suspected data compromise.

B. Incident Response Steps:

1. Remove all network access from the machine immediately (remove network cables or air card, power the machine off using the power button, unplug the power cable, etc.).

2. Contact IT in person, via email or phone:
    a. Email: [redacted]
    b. Call List:
        i. Network Administrator – Office: 951-955-4257; Cell: 951-377-5653;
        ii. IT Manager – Office: 951-955-0700; Cell: 951-515-4921.

3. IT staff shall document the following:
    a. Name and title of the person contacting IT;
    b. Time of the contact;
    c. Contact information for the person contacting IT;
    d. Nature of the incident;
    e. Equipment involved;
    f. Location of the equipment;
    g. Whether the equipment is critical to the operation of the department;
    h. Name/IP Address of affect equipment;
    i. How the issue was detected;
    j. When the issue was first noticed.

4. IT staff shall determine the following:
    a. Severity of the incident;
    b. Urgency of response;
    c. Whether the incident is real or perceived;
    d. Whether the issue is still ongoing;
    e. What kind of data is at risk;
    f. Whether CLETS/SmartJustice data was compromised;
    g. Whether there would be an operational impact should the attack succeed;
    h. Whether the incident is coming from inside or outside the trusted network;
    i. Type of the incident;
    j. Response level.

5. IT staff shall take the following actions:
    a. Mitigate the issue;
    b. Provide the Chief Probation Officer and the Human Resources Division Director with a report of the incident, to include:
        i. Cause of incident

ii. Type of incident
iii. How issue was resolved
iv. Any mitigating issues
v. Recommendations

c. Preserve any evidence (event logs, emails, etc.);
d. Assess any damages or costs;
e. Review response and procedures;
f. Implement recommendation upon written approval.

6. The Human Resources Division Director will notify the following external agencies if required:
    a. DOJ;
    b. CLETS Host Agency;
    c. Affected persons if personal information was compromised.