CJIS Security

703.1 CJIS SECURITY REQUIREMENT

The San Diego County Probation Department is a CLETS Subscribing Agency and must adhere to the requirements established in the California Law Enforcement Telecommunications System Policies, Practices, and Procedures (CLETS PPP) and the FBI CJIS Security Policy. It is the responsibility of the Agency CLETS Coordinator (ACC) to ensure, annually, the requirements of the CLETS PPP and FBI CJIS Security Policy are reviewed to ensure the department is still in compliance. The CLETS policies can be found on the California Law Enforcement Website at https://clew.doj.ca.gov. The latest FBI CJIS Security Policy can be found online at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

703.2 SECURITY AWARENESS TRAINING

Security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have physical and logical access to CJI and all personnel who have unescorted access to a physically secure location. Records of individual security awareness training and specific information system security training shall be documented, kept current, and maintained by the ACC.

703.3 ACCOUNT MANAGEMENT

Access to the Probation Department and CORI/CLETS information systems shall be granted based on a valid need-to-know/right-to-know basis which is determined by assigned official duties and the satisfaction of all personnel security criteria. The Probation Information Technology Division shall be notified immediately when a user's information system usage or need-to-know or right-to-know changes, when a user is terminated or transferred, or associated accounts are removed or disabled.

703.4 AUTHENTICATION

All personnel who are authorized to store, process, and/or transmit CJI shall be uniquely identified and may include the employee's ID, part of a full name, or other unique alphanumeric identifiers. Password standards for all information systems shall follow the Basic or Advanced Password Standards as outlined in the FBI CJIS Security Policy.

703.5 REMOTE ACCESS

All methods of remote access to the Probation Department and CORI/CLETS information shall be authorized, monitored, and controlled utilizing automated managed access control. Remote access may be permitted for privileged functions and only for compelling operational needs.

703.6 PERSONALLY OWNED INFORMATION SYSTEMS

Personally owned information systems and mobile devices shall not be authorized to access, process, store, or transmit CJI. If personally owned mobile devices (i.e., Bring Your Own Device

[BYOD]) are authorized, they shall be controlled in accordance with the FBI CJIS Security requirements and the County of San Diego Administrative Manual Section 0400-09 Employee Bring Your Device (BYOD) Acceptable Use Policy.

703.7 PUBLICLY OWNED INFORMATION SYSTEMS

Publicly owned information systems shall not be authorized to access, process, store, or transmit CJI. Publicly accessible computers include, but are not limited to, hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

703.8 DISSEMINATION OF CORI INFORMATION

Electronic, automated, and paper copies of California Criminal History (CORI) shall only be disseminated to persons and agencies authorized by law. CORI released to outside agencies that are currently not a CLETS Subscribing Agency must follow requirements outlined in the FBI CJIS Security Policy and the CLETS policies found on the CLEW website.

The release of information from the CLETS by a CLETS subscribing agency is authorized on a need-to-know, right-to-know basis. In accordance with the CLETS Policies, Practices, and Procedures (PPP) section 1.5.3, and before the release of information from the CLETS, the following must be completed, agreed to by both agencies, and approved by the California Department of Justice (CA DOJ). A statute, ordinance, or regulation must exist that requires the governmental agency to perform a law enforcement-related function, which necessitates receiving information from the CLETS.

Data sharing agreements shall be in place with agencies accessing or receiving CORI/CLETS information and shall be reviewed and approved by the Agency CLETS Coordinator, County Counsel, and the Chief Probation Officer.

703.9 ANNUAL MISUSE REPORTING

Misuse of CORI/CLETS information systems shall be tracked on an ongoing basis and reported through the Chain of Command. Annual system misuse must be reported to the CA DOJ by February 1st of each year, for the prior calendar year, even if no misuse occurred.

703.10 INCIDENT RESPONSE

All members are required to report security events and incidents as quickly as possible to the Probation Information Technology Division and Chain of Command.

The County Technology Office and Chief Information Security Officer (CISO) have developed the Incident Response Procedure which also ensures the protection of CJI. The Incident Response Procedure establishes operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; and tracks, documents, and reports incidents to appropriate agency officials and/or authorities.

703.11 ROLES AND RESPONSIBILITIES

703.11.1 AGENCY CLETS COORDINATOR (ACC)

The Agency CLETS Coordinator (ACC) is an employee designated by the Probation Department to serve as the coordinator with the Department of Justice (DOJ) on matters pertaining to the use of CLETS, National Crime Information Center (NCIC), National Law Enforcement Telecommunication System (NLETS) and the DOJ criminal justice databases. The ACC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

Responsibilities include:

(a) Management of User Accounts

(b) Maintenance and Storage of Employee/Volunteer Statement Forms and CJIS Security Addendums

(c) Maintenance and Storage of DOJ-mandated agreements, including Release of Information, Management Control Agreements, and Private Contractor Management Control Agreements

(d) A "Third Party Log" must be maintained for all Criminal History Information released to an outside agency that is not a CLETS Subscribing Agency

(e) Ensuring the Third-Party Release Log for CORI with regard to information released to other agencies is completed and accurate

(f) Ensuring compliance with mandated state and federal auditing requirements

(g) Oversee proper distribution of policy or database change information

(h) Ensuring compliance with CLETS, CJIS, NCIC, and NLETS policies and regulations

(i) Ensuring CLETS terminals, equipment and messages are secure from unauthorized access

(j) Determine the need for CLETS training and coordinate the training

(k) Maintain CLETS/NCIC training records

Annually request a complete list from the Personnel Division of all sworn and professional staff including position titles to validate all CLETS system account access. The ACC additionally receives daily PeopleSoft emails for all new hires, transfers, retirements, and terminations. These emails are used daily to activate, modify, review, disable and remove CLETS access.

703.12 SECURITY POINT OF CONTACT (SPOC)

The responsibility for the technical security of all automated systems shall rest with the Security Point of Contact (SPOC) for the technical security of all automated systems. The ACC or Chief Information Security Officer (CISO) can serve as the SPOC and shall furnish the Probation Department with regulations adopted by the County Information Security Officer (CISO) to show that the computerized system is secure from unauthorized access, alteration, deletion, or release.

703.13 CHIEF INFORMATION SECURITY (CISO)

The County Technology Office (CTO) will designate a Chief Information Security Officer (CISO), as the security point of contact (SPOC) with the DOJ and is responsible for technical compliance with the CJIS Security Policy to ensure confidentiality, integrity, and availability of criminal justice information to the Probation Department. The CISO aids with implementing security-related controls for the department and its users. The CISO shall establish a security incident response and reporting procedure to discover, investigate, document, and report to the affected criminal justice agency and the FBI CJIS Division any major incidents that significantly endanger the security or integrity of CJI.

703.14 LOCAL AGENCY SECURITY (LASO)

The ACC shall serve as the LASO to identify who is using approved hardware, software, and firmware and ensures no unauthorized individuals have access to the same and shall identify and document how equipment is connected to the CLETS system. The LASO shall ensure that member security screening procedures are being followed, ensure the appropriate security measures are in place and working as expected, and shall support policy compliance and properly document any security incidents.

703.15 REFERENCES

(a) For further guidance, please refer to the latest FBI CJIS Security Policy which can be found on the FBI.gov website.

(b) California Law Enforcement Telecommunications System Policies, Practices, and Procedures (CLETS PPP) can be found on the CLEW website at https://clew.doj.ca.gov.

(c) Policy 324 Information Technology Use

(d) Policy 348 Confidentiality & Probation Case Files

703.16 ATTACHMENTS

The following DOJ forms can be found on the CLEW website at https://clew.doj.ca.gov:

(a) HDC 0001 CLETS Subscriber Agreement

(b) HDC 0002 Change Request

(c) HDC 0003 ACC Responsibilities

(d) HDC 0004A Management Control Agreement

(e) HDC 0004B Private Contractor Management Control Agreement

(f) HDC 0005 Interagency Agreement

(g) HDC 0006 Release of Information from the CLETS

(h) HDC 0007 Reciprocity Agreement

(i) HDC 0008 MSD-Users Costs and Requirements

(j) HDC 0009 Employee-Volunteer Statement Form

(k) HDC 0010 CLETS Misuse Investigation Reporting Form

(l) HDC 0011 CA DOJ Security Point of Contact Delineation and Agreement

(m) HDC 0012 FBI CJIS Security Addendum