CJIS Security

703.1 PURPOSE AND SCOPE

The purpose of this policy is to provide the appropriate protection and control of criminal justice information (CJI). The policy applies to all members - employees, contractors, providers, volunteers, noncriminal justice agency representatives, or members of a criminal justice agency

—with direct or indirect access to, or who operate in support of, criminal justice services and information.

703.2 DEFINITIONS

California Law Enforcement Telecommunications System (CLETS): The computerized telecommunications system in the State of California that is used by public agencies of law enforcement and criminal justice for accessing law enforcement information and sending law enforcement messages.

Criminal Justice Information (CJI): Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS-provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/ incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

Criminal Justice Information Services Division (FBI CJIS or CJIS): The FBI division is responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Criminal Offender Record Information (CORI): CORI is defined as criminal history arrest information regarding a subject or subjects retained by/at any governmental entity therein is considered CORI and falls under the CORI rules and regulations.

703.3 POLICY

It is the policy of the San Diego Probation Department to adhere to the FBI CJIS Security Policy and maintain the minimum standards as outlined in the CJIS Security Procedure. The scope of this policy applies to any electronic or physical media containing CJI and the appropriate security controls from the creation to dissemination, whether at rest or in transit. The CJIS Security Policy guides the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. In addition, this policy applies to any authorized person who accesses, stores, and/or transports electronic or physical media containing CJI.

703.4 REFERENCES

(a) For further guidance, please refer to the latest FBI CJIS Security Policy which can be found online at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

(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