SAN BERNARDINO COUNTY
PROBATION DEPARTMENT PROCEDURE

COMPUTER INFORMATION SECURITY/USER SIGN-ON & ACCESS CONTROLS

Authority:
Tracy Reece, Chief Probation Officer

Purpose:
To establish guidelines regarding computer information security in daily operations.

Definitions:
Automated Systems: The custodian of data, information, and technology assets owned by the Department who creates and executes instructions for collecting, processing, and distributing data and information.

Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division: Provides law enforcement, national security, and the intelligence community with criminal justice information. The CJIS Security Policy sets minimum-security requirements for any organization accessing the data, as well as guidelines to protect the transmission, storage, and creation of criminal justice information (CJI) such as fingerprints, identity history, case/incident history, etc. CJIS standards include best practices in areas like data encryption, wireless networking, and remote access, as well as multi-factor authentication, and physical security. All entities, whether law enforcement or a non-criminal justice agency that has access to any of the FBI's CJI data must adhere to the security standards.

Criminal Offender Record Information (CORI): Records and data compiled by criminal justice agencies for purposes of identifying criminal offenders. CORI may include a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, and information on sentencing, incarceration, rehabilitation, and release. Criminal justice agencies throughout the state provide this information to the Department of Justice (DOJ), which in turn is required to maintain it in a statewide repository. CORI is privileged and confidential, and may not be disclosed except as specifically authorized by law.

User Identification (ID): A means of authenticating each authorized user of the department's network. Each authorized user has a unique and separate User ID. Each user will choose a password which is the key that verifies a user is who they say they are. Passwords authenticate users with their User ID for access to the network. Passwords will be complex (i.e. minimum password length, including upper and lower case alpha, numeric, special characters, and the inability to use the same password in a designated period of time/resets). The combination of the User ID and password provides accountability for a user's actions while using the network.

Main Distribution Frame Room (MDF): A room that houses a cable rack(s) that interconnects and manages the telecommunications wiring between itself and any number of Intermediate Distribution Frame (IDF) Room(s). Unlike an IDF, the MDF connects private or public lines coming into a building with the internal network.

Intermediate Distribution Frame Room (IDF): A room that houses cable rack(s) that interconnects and manages the telecommunications wiring between an MDF and distal

workstation devices. Cables entering a building run through a centralized MDF, then to each individual IDF, and then on to specific workstations.

Responsibilities:

I. Automated Systems:
   A. Ensure protection of data and information while it is processed or stored on the central computers.
   B. Ensure data is recoverable and restorable in the event of damage or loss, including the development of business contingency plans.
   C. Control the rate of technology introduction as well as the types and scale of technologies.

II. Department Information Services Administrator (DISA)/Designee:
   A. Provide guidelines to Probation personnel on the appropriate use of Probation information.
   B. Ensure adequate controls protect information from accidental or deliberate disclosure, damage, misuse, or loss.
   C. Monitors compliance with this procedure on an ongoing basis in the normal course of business.
   D. Assess, document, and take appropriate action upon receiving reported violations and circumvention of safeguards.
   E. Maintains access to MDF/IDF Rooms:
      1. Maintain and control the list of authorized personnel who have access to the MDF/IDF rooms, either via direct access in the room where equipment is physically located, or remote access.
      2. Review and update the access list on a semi-annual basis or as staff assignments dictate.
      3. Determine and approve access on a business "need to know, right to know" basis.
      4. Ensure keys/access rights are given to only those persons on the list.
      5. Ensure an authorized escort is present at all times when deemed appropriate when a person not on the list (e.g. Facilities Management, Innovation Technology Department) is present in the room.

III. Probation Employees:
   A. Create, maintain, and safeguard information in a secure environment.
   B. Protect data from unauthorized modification, destruction, or disclosure, whether accidentally or intentionally.
   C. Comply with established safeguards to protect information residing on the central computer files.
   D. Protect Probation information and comply with policies, standards, and procedures governing its use.
   E. Not access any location (MDF/IDF) or information not legally entitled to by virtue of employment or in any way compromise the security of the information system. When handling information, must have a "need to know, right to know," and be authorized by Management to access the information.
   F. Ensure the door remains locked in MDF and IDF rooms at all times.
   G. Use Probation computing resources in conformance with all County and Department policies and procedures.
   H. Promptly report a compromise or circumvention of any safeguards to the DISA/designee.

I. Not store or maintain copies of any CJI or CORI on any personal or department-issued devices (laptop, tablet, iPad, smartphone, etc.). Examples of this may include but are not limited to copies of Caseload Explorer (CE) data, an overview sheet, CE reports, or any agency CJI data, etc. This includes printed copies of offender data derived from any CJI system.
J. Shall be responsible for all actions resulting from their User ID and password.
K. Shall not share User ID and password directly (by providing the information) or indirectly (by logging in and permitting others to use the system) with anyone, including other probation employees, consultants, or contractors as well as persons not employed by or in contract with the Probation Department.
L. Shall sign a computer/software user agreement.

Guidelines:

A. The improper use of Department information systems and networks may be considered cause for disciplinary action up to and including termination. The following are examples of misuse that could result in revocation of access privileges or other disciplinary action:
   1. Accessing confidential information for personal purposes.
   2. Sending Probation proprietary or confidential information to anyone not entitled to know or possess such information.
   3. Intentionally disrupting network service.
   4. Political activities.
   5. Personal activities that incur additional costs to Probation or interfere with a user's work performance.
B. Employee computer usage is routinely monitored as part of the Probation Information Systems Security Program.
C. All MDF/IDF rooms are monitored through closed-circuit camera systems. There shall be no expectation of privacy when accessing these locations.
D. Probation network services and facilities are provided to support the day-to-day business activities of the Probation Department and those external entities that have an established business partnership with the Department.
E. Any compromise of computer security and/or access may result in consequences up to and including immediate termination, criminal and civil prosecution relative to all applicable County statutes, California, and Federal laws.

Inspections:

Refer to the Policy and Procedure Inspection Matrix.

Foundation:

Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
Copyright Act of 1976
Criminal Justice Information Services Security Policy
Foreign Corrupt Practices Act of 1977

References:

Procedures:
CLETS (California Law Enforcement Telecommunications System): Incident Response Plan
Electronic Communications
Employee Responsibility—Code of Conduct
Maintaining CJIS Compliance While Working Remotely
Offender Record Security

Replaces:
Computer Server Room Access
Computer Sign-On/User Access Controls
Computer Systems and Data Security

Issued By: Tracy Reece, Chief Probation Officer

Original Issue Date: March 22, 2006

Revised: February 21, 2020
Revised: July 25, 2022