5.3.21 Data Security

(a) Introduction and Overview

(1) California Department of Corrections and Rehabilitation (CDCR), California Correctional Health Care Services (CCHCS), and California Prison Industry Authority (CALPIA), hereinafter referred to as department, collects, processes, transmits, and stores large amounts of data to support essential missions and business functions. Some data maintained by the department may be sensitive or confidential, and may require special precautions to protect it from unauthorized modification, or deletion as per the State Administrative Manual.

(2) The department has the responsibility to classify its data and information assets, and to implement suitable controls to protect it from unauthorized access, corruption, or loss.

(b) Objectives

The primary objective for this policy is to define department requirements to manage the confidentiality, integrity, and availability of department data and information assets throughout their lifecycles: from collection, creation, storage, and use, to destruction and disposal.

(c) Scope and Applicability

(1) The scope of this policy extends to all state and agency data and information assets owned or operated by the department, and operated by third parties on behalf of the department, and governs all state and department data and information assets in all forms and media types, including digital and physical formats.

(2) This policy applies to all department personnel.

(d) Policy Directives

The department shall:

(1) Ensure that roles and responsibilities for the identification, classification, and life cycle management of all department data and information assets are defined, documented, and implemented.

(2) Ensure that all department information assets, including information and information systems, are categorized according to their criticality, as well as their sensitivity and susceptibility to inadvertent damage, loss, or exposure and corresponding impact to the department.

(3) Ensure that methods to protect the confidentiality, integrity, and availability of department data and information assets according to their classification are defined, documented, and implemented.

(4) Ensure that conditions for access to and use of department information assets for all personnel are defined and documented.

(5) Ensure that all personnel with access to department data and information assets are trained regarding data access and handling according to their roles and responsibilities.

(6) Ensure that department data and information assets are used solely for their intended purpose.

(7) Ensure that department data and information assets are securely destroyed and disposed of once they are no longer required by the department.

(8) Ensure that the proper authorities are notified of data security incidents as required.

(e) Roles and Responsibilities

(1) Department Chief Information Officer (CIO) or Designee

(A) The CIO or designee owns this policy and is responsible for ensuring that all users of department information assets are aware of this policy and acknowledge their individual responsibilities.

(B) The CIO or designee is responsible for ensuring that this policy is reviewed annually and updated accordingly.

(C) The CIO or designee is required to audit and assess compliance with this policy at least once every two years.

(2) Department Information Security Officer (ISO)

(A) The ISO shall assist Owners of Information Assets and Information Asset Custodians in the identification of data security controls and processes.

(B) The ISO shall participate in incidents involving data security.

(C) The ISO shall ensure that data security controls, methods and processes meet department and applicable regulatory requirements for security and privacy.

(3) Department Owners of Information Assets and Program Management

(A) Owners of Information Assets shall ensure that this policy is implemented and reviewed annually, and updated as necessary.

(B) Owners of Information Assets shall ensure that roles and responsibilities for the identification, classification, and life cycle management of all data and information assets under their purview are defined, documented and implemented.
(C) Owners of Information Assets shall ensure confidentiality and integrity controls commensurate with asset classification are implemented for data and information assets under their purview.
(D) Owners of Information Assets shall ensure that conditions and rules for access, availability, and use of data and information assets under their purview are commensurate with asset classification.

(4) Department Information Asset Custodians
(A) Information Asset Custodians shall assist Owners of Information Assets in identifying data security controls commensurate with the classification of the data.
(B) Information Asset Custodians shall document, implement, monitor, and maintain data security protection controls as defined by Owners of Information Assets.
(C) Information Asset Custodians shall develop and implement tools, technologies, processes, and procedures to support, monitor and maintain data security controls.
(D) Information Asset Custodians shall notify respective Owners of Information Assets and the department Information Security Officer (ISO) and the Privacy Officer of all security incidents pertaining to the security of department data, particularly if the incident is related to personally identifiable information (PII).
(E) Information Asset Custodians shall maintain data security records as defined by Owners of Information Assets commensurate with the classification of the data.

(5) Department Users
Users of department information assets shall be aware of and adhere to all department information security and privacy policies.

(f) Enforcement

(1) Non-compliance with this policy may result in disciplinary or adverse action as set forth in the Department Operations Manual, Chapter 3, Article 22.
(2) The department shall comply with the information security and privacy policies, standards and procedures issued by the California Department of Technology (CDT), Office of Information Security (OIS). In addition to compliance with the information security and privacy policies, standards, procedures, and filing requirements issued by the OIS, the department shall ensure compliance with all security and privacy laws, regulations, rules, and standards specific to and governing the administration of their programs. Program administrators shall work with their general counsel, ISO, and Privacy Program Officer or Coordinator to identify all security and privacy requirements applicable to their programs and ensure implementation of the requisite controls.
(3) The consequences of negligence and non-compliance with state laws and policies may include department and personal:
(A) Loss of delegated authorities.
(B) Negative audit findings.
(C) Monetary penalties.
(D) Legal actions.

(g) Auditing

(1) The department has the right to audit any activities related to the use of state information assets.
(2) CDT OIS and the department have the statutory right to audit department readiness to respond and recover from an incident.

(h) Reporting

Violations of this policy shall be reported to the department ISO.

(i) Security Variance Process

If compliance is not feasible, or if deviation from this policy is necessary to support a business function, the respective manager shall formally request a security variance as defined by the ISO.

(j) Authority

This policy complies with State of California Government Code Section 11549.3.

(k) Revisions

The CIO or designee shall ensure that the contents of this article are current and accurate.

References

- Statewide Information Management Manual 5305-A, Information Security Program Management Standard
- State Administrative Manual, Section 5305.5, Information Asset Management
- State Administrative Manual, Section 5310.4, Individual Access to Personal Information
- State Administrative Manual, Section 5310.6, Data Retention and Destruction
- State Administrative Manual, Section 5310.7, Security safeguards
- State Administrative Manual, Section 5340, Information Security Incident Management
- State Administrative Manual, Section 5340.1, Incident Response Training
- State Administrative Manual, Section 5340.2, Incident Response Testing
- State Administrative Manual, Section 5340.3, Incident Handling
- State Administrative Manual, Section 5340.4, Incident Reporting
- State Administrative Manual, Section 5350, Encryption
- State Administrative Manual, Section 5365, Physical access
- State Administrative Manual, Section 5365.1, Access Control for Output Devices
- State Administrative Manual, Section 5365.2, Media Protection
- State Administrative Manual, Section 5365.3, Media Disposal
- Federal Information Processing Standard, FIPS 199
- National Institute of Standards and Technology, Special Publications 800-53, Access Control, AC-3, AC-4
- National Institute of Standards and Technology, Special Publications 800-53, Audit and Accountability, AU-2, AU-3, AU-13
- National Institute of Standards and Technology, Special Publications 800-53, Configuration Management, CM-8
- National Institute of Standards and Technology, Special Publications 800-53, Media Protection, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7
- National Institute of Standards and Technology, Special Publications 800-53, Physical and Environmental Protection, PE-5, PE-19, PE-20
- National Institute of Standards and Technology, Special Publications 800-53, Planning, PL-4
- National Institute of Standards and Technology, Special Publications 800-53, Program Management, PM-9
- National Institute of Standards and Technology, Special Publications 800-53, Risk Assessment, RA-2, RA-3
- National Institute of Standards and Technology, Special Publications 800-53, Security Assessment and Authorization, CA-7
- National Institute of Standards and Technology, Special Publications 800-53, System and Communications Protection, SC-4, SC-8, SC-13, SC-17, SC-28
- National Institute of Standards and Technology, Special Publications 800-53, System and Services Acquisition, SA-11
- National Institute of Standards and Technology, Special Publications 800-53, System and Information Integrity, SI-12
- California Department of Corrections and Rehabilitation, Department Operations Manual Chapter 3, Article 22
- California Department of Corrections and Rehabilitation, Department Operations Manual Chapter 4, Article 45, Section 49020.6, 49020.6.1, 49020.6.2
- California Department of Corrections and Rehabilitation, Department Operations Manual Chapter 4, Article 46, Section 49030.4
- California Government Code Section 11549.3

Revision History
Effective: 11/30/2022