5.3.18 Security Assessment and Authorization

(a) Introduction and Overview

(1) California Department of Corrections and Rehabilitation (CDCR), California Correctional Health Care Services (CCHCS), and California Prison Industry Authority (CALPIA) is responsible for the integration of information security and privacy within the organization. This includes, but is not limited to, the design and early identification of appropriate security controls in information asset acquisitions, in the design of new systems, or existing systems that are undergoing substantial redesign, including both in-house and outsourced solutions.

(2) The CDCR, CCHCS, and CALPIA (hereinafter referred to as department) shall ensure its Information Security Officer (ISO) and, where applicable, its Privacy Program Coordinator and Technology Recovery Coordinator, are actively engaged with both the owners of information assets, and any relevant project, procurement, and technical personnel, to identify and implement the appropriate security controls required to manage risk to acceptable levels. Where applicable, the department ISO shall also work with other stakeholders, as appropriate.

(b) Objectives

The objective for this policy is to establish a documented security assessment and authorization plan.

(c) Scope and Applicability

(1) The scope of this policy extends to all State and Agency information assets owned or operated by the department.

(2) This policy applies to the department ISO, Privacy Officer, Privacy Program Coordinator, program management, Owners of Information Assets and Information Asset Custodians.

(d) Policy Directives

The department shall ensure that a plan for assessing security controls in department information assets is defined and documented. The plan shall include the following:

(1) Roles and responsibilities for security assessments and authorization.

(2) Assessments are integrated in life cycle processes and operational assessments, and identify weaknesses and deficiencies early in information asset acquisition, development, and integration processes.

(3) Essential information needed to make risk management decisions as part of security authorization processes is provided to the defined risk decision makers.

(e) Roles and Responsibilities

(1) The department Chief Information Officer (CIO) or Designee:

(A) 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) Is responsible for ensuring that this policy is reviewed annually, and updated accordingly.

(C) Is required to audit and assess compliance with this policy at least once every two years.

(2) The department Information Security Officer (ISO) shall facilitate security assessments and authorizations, and shall provide advice as appropriate.

(3) The department Owners of Information Assets and Program Management in collaboration with Information Asset Custodians shall:

(A) Ensure that this policy is implemented and shall review the policy's implementation annually.

(B) Ensure requisite security controls are implemented in accordance with applicable security requirements and documented authorizations for information assets.

(C) Ensure that any security control gaps and residual risks being accepted are formally documented.

(D) Ensure that records and results of assessments and risk decisions are maintained.

(E) Ensure that records and results of assessments and risk decisions are provided to information security officers in a timely manner.

(4) The department Information Asset Custodians shall implement the requisite security controls based upon the sensitivity or criticality of the assets as defined by the owners of information assets.

(5) The department Privacy Officer/Privacy Program Coordinator shall ensure that privacy threshold and privacy impact assessments are completed as part of the security assessment and authorization process.

(f) Enforcement

(1) Non-compliance with this policy may result in disciplinary or adverse action as set forth in 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 department ISO.

(j) Authority

This policy complies with 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, Section 5305-A, Information Security Program Management Standard
- State Administrative Manual, Section 5305.7, Risk Assessment
- State Administrative Manual, Section 5315, Information Security Integration
- State Administrative Manual, Section 5315.9, Security Authorization
- National Institute of Standards and Technology, Special Publications 800-53, Asset, Authorization, and Monitoring, (CA), CA-1, CA-2, CA-4, CA-6
- National Institute of Standards and Technology, Special Publications 800-53, System and Information Integrity Policy and Procedures (SI), SI-1, SI 6, SI-12
- National Institute of Standards and Technology, Special Publications 800-37, Risk Management Framework for Information Systems and Organizations: A Systems Life Cycle Approach for Security and Privacy
- 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, Sections 49020.9
- California Government Code, Section 11549.3

Revision History

Effective: 03/2022