

5.3.25 Security and Privacy Awareness Training

(a) Introduction and Overview

A well-trained workforce, aware of information privacy and security risk, plays a crucial role in protecting organizations against a variety of information security threats. Consequently, a formal privacy and security awareness training program is a key component of California Department of Corrections and Rehabilitation (CDCR), California Correctional Health Care Services (CCHCS), and California Prison Industry Authority (CALPIA)'s, hereinafter referred to as department, information security program.

(b) Objectives

Objectives for this policy are to establish the requirement of a formal and effective department privacy and security awareness and training program for all department personnel.

(c) Scope and Applicability

The scope of this policy applies to all department personnel and governs all forms of access to department information assets.

(d) Policy Directives

The department shall:

- (1) Establish a formal department privacy and security awareness training program, with clearly defined roles and responsibilities, designed to be delivered to all personnel with access to department information assets.
- (2) Provide privacy and security awareness training to all personnel upon commencement of their employment with the department, and on an annual basis thereafter.
- (3) Ensure role-based privacy and security awareness training content is delivered commensurate with personnel roles and responsibilities.
- (4) Ensure effectiveness of the security awareness program through a process of tracking and reporting metrics.
- (5) Maintain individual records of all security and privacy training undertaken annually by department personnel for a period of three years or as defined in the records retention schedule.

(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 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)

The ISO shall ensure the development implementation, and compliance of the department's security awareness training program.
- (3) Department Privacy Officer
The Privacy Officer shall ensure the development, implementation, and compliance of the department's privacy awareness training program.
- (4) Department Users
 - (A) Users shall participate in all required privacy and security awareness training annually.
 - (B) Users 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.

CALIFORNIA DEPARTMENT OF CORRECTIONS AND REHABILITATION
CALIFORNIA CORRECTIONAL HEALTH CARE SERVICES
Health Care Department Operations Manual

- (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

- (1) The department Information Security Officer (ISO), Chief Privacy Officer or Coordinator and Training Coordinator shall provide department program management with regular reports on personnel participation in, and the effectiveness of privacy and security and awareness training.
- (2) 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

- State Administrative Manual, Section 5305.3, Information Security Roles and Responsibilities
- State Administrative Manual, Section 5320, Training and Awareness for Security and Privacy
- State Administrative Manual, Section 5320.1, Security and Privacy Awareness
- State Administrative Manual, Section 5320.2, Security and Privacy Training
- State Administrative Manual, Section 5320.3, Security and Privacy Training Records
- State Administrative Manual, Section 5320.4, Personnel Security
- National Institute of Standards and Technology, Special Publications 800-53, Planning, PL-4
- National Institute of Standards and Technology, Special Publications 800-53, Awareness and Training, AT-1, AT-2, AT-3, AT-04
- 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 41, Section 48010.5
- California Department of Corrections and Rehabilitation, Department Operations Manual Chapter 4, Article 45, Sections 49020.4, 49020.7.2, 49020.7.3, 49020.7.3.1
- California Government Code Section 11549.3

Revision History

Effective: 11/30/2022