5.3.17 Physical and Environmental Protection

(a) Introduction and Overview

(1) Information assets owned by the California Department of Corrections and Rehabilitation (CDCR), California Correctional Health Care Services (CCHCS), and California Prison Industry Authority (CALPIA) (including but not limited to department data and information, servers, laptops, tablets, cell phones, and removable storage devices) are strategic assets intended for official business use, and they are entrusted to State personnel in the performance of their job related duties.

(2) Restricting physical access to information assets reduces the potential for their damage and misuse. Implementing and maintaining environmental controls provides optimal operating conditions for information assets that are critical to CDCR, CCHCS, and CALPIA (hereinafter referred to as department) business functions.

(b) Objectives

Objectives for this policy are to establish physical security and environmental protection control requirements to safeguard department information assets against unauthorized access, use, disclosure, disruption, modification, or destruction.

(c) Scope and Applicability

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

(2) This policy applies to all department personnel.

(d) Policy Directives

(1) The department shall define the control requirements for the physical environmental protection of information assets.

(2) The department shall implement, manage, monitor, and regularly maintain physical security and environmental protection controls to safeguard State information assets for which they have custodianship.

(3) Personnel identification systems and facility access controls shall be implemented for all personnel and visitors. Access logs shall be reviewed at minimum annually.

(4) Environmental controls shall be implemented in computer rooms and data centers, including but not limited to, temperature and humidity regulators, fire detection and suppression, and electrical power conditioning.

(5) Supporting controls, processes, and procedures to control physical access (e.g., security gates), handling digital media, and emergency processes and procedures shall be implemented.

(6) Service records of periodic maintenance of physical and environmental protection controls (e.g., heating/cooling unit servicing) and results of tests of environmental controls (e.g., power outage) shall be retained for a minimum of six months.

(7) Security risks shall be identified, remediated, and reported to the department Information Security Officer (ISO).

(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 Owners of Information Assets and Program Management:

(A) Shall formally approve and authorize access and revocation of access to information assets.

(B) In collaboration with the Information Asset Custodians shall validate access to information assets under their purview on an annual basis, or when staffing, resource or job function changes occur.

(C) In collaboration with the Information Asset Custodians shall validate protection requirements for information assets under their purview on an annual basis.

(3) The department Information Asset Custodians:

(A) In collaboration with the Owners of Information Assets shall define protection requirements for information assets under their purview.

(B) Shall implement, manage, maintain, monitor, and periodically test physical and environmental protection controls to safeguard State information assets for which they have custodianship and as defined by the respective Owners of Information Assets.

(C) Shall track and monitor all access to information assets, including physical access, as defined by Owners of Information Assets, and physical and environmental controls to validate correct operation.
(D) Shall maintain all maintenance records and results of periodic tests.

(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 CDT 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 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 5325, Business Continuity Planning
- State Administrative Manual, Section 5360, Identity and Access Management
- State Administrative Manual, Section 5365, Physical Security
- National Institute of Standards and Technology, Special Publications 800-53, Physical and Environmental Protection, PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-16, PE-17
- National Institute of Standards and Technology, Special Publications 800-53, Maintenance, MA-1, MA-2, MA-3, MA-4, MA-5
- National Institute of Standards and Technology, Special Publications 800-53, Contingency Planning, CP-2, CP-3
- National Institute of Standards and Technology, Special Publications 800-53, Incident Response, IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7
- 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
- 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 49020.9, 49020.10
- California Government Code, Section 11549.3

Revision History
Effective: 03/2022