5.3.10 Change and Configuration Management

(a) Introduction and Overview

(1) Business functions are highly dependent on secure and stable Information Technology (IT) operating environments. Secure and reliable IT environments are enabled through both maintaining standard configurations and establishing processes and procedures to effectively manage changes to the operating environments.
(2) The goal of formalized IT change management is to facilitate IT changes as defined in enterprise standards, guidelines, and procedures while minimizing negative impacts to the organization.
(3) The goal of IT configuration management is to establish, implement, and manage information asset baseline configurations and maintain consistency throughout the system lifecycle.
(4) This policy establishes California Department of Corrections and Rehabilitation, California Correctional Health Care Services, and California Prison Industry Authority (hereinafter referred to as department) requirement for formal change and configuration management.

(b) Objectives

The objective for this policy is to establish department requirements for standardized methods and procedures for the management of information asset configurations and changes to department information and technology environments, while integrating security and risk considerations.

(c) Scope and Applicability

(1) The scope of this policy extends to all State information assets owned and operated by the department, information assets managed by third parties on behalf of the department, and all information assets that process or store department information in support of department services and mission.
(2) This policy applies to Owners of Information Assets and Information Asset Custodians.

(d) Policy Directives

The department shall:
(1) Formally manage all changes to information assets.
(2) Utilize the Change Control Board, which includes a change advisory board that meets on a regular basis to review changes to information assets.
(3) Ensure that the change advisory board comprises representation from appropriate stakeholders, and in particular from impacted business areas.
(4) Ensure that the change advisory board includes formal security representation, and that change management processes formally integrate security evaluations and risk impact assessments in all change activities.
(5) Establish comprehensive enterprise-wide change management, comprised of supporting processes, workflows, and a centralized repository for all changes, including changes to baseline configurations.
(6) Establish, implement, and manage department operating baselines for information asset configurations.
(7) Establish and implement technologies, processes, and procedures to maintain and manage information asset configurations.
(8) Ensure third parties and contractors are subject to change and configuration management policies, discipline, and practices. Any changes to department information assets proposed by service providers, regardless of whose environment they operate in, shall be governed by department change and configuration management processes.

(e) Roles and Responsibilities

(1) Department Chief Information Officer (CIO) or Designee:
(A) Owns this policy and is responsible for ensuring that all Owners of Information Assets, Information Asset Custodians, and 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 2 years.
(2) Department Information Security Officer (ISO):
(A) Shall assist Owners of Information Assets and Information Asset Custodians in the identification of data security controls and processes.
(B) Shall ensure that data security controls, methods, and processes meet department and applicable regulatory requirements for security.

(3) Department Owners of Information Assets and Program Management:
In collaboration with the Information Asset Custodians shall ensure that this policy and its directives are implemented and enforced.
(4) Department Information Asset Custodians:
(A) Shall implement configuration and change management technology, process, and workflow controls as approved by Owners of Information Assets.
(B) Shall maintain change and configuration management records for a minimum period of 12 months. Secure deletion or destruction of these records shall be in accordance with the records retention schedule.

(f) Enforcement

(1) Non-compliance with this policy may result in disciplinary or adverse action as set forth in California Department of Corrections and Rehabilitation, 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 the 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, 19C, Project Approval Lifecycle Stage 3 – Solution Development
- Statewide Information Management Manual, Sections 58C, 58D, 66B, 5305-A, 5310-A and B; 5325-A and B; 5330-A, B, and C; 5340-A and C; and 5360-B
- State Administrative Manual, Section 5315, Information Security Integration
- State Administrative Manual, Section 5315.5, Configuration Management
- State Administrative Manual, Section 5355, Endpoint Defense
- National Institute of Standards and Technology, Special Publications 800-53, Configuration Management, CM-2, CM-3, CM-4, CM-5, CM-6, CM-9
- 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
- California Government Code, Section 11549.3

Revision History
Effective: 02/2022