5.3.26 Software Management and Licensing

(a) Introduction and Overview

(1) State entities are required to establish and maintain an inventory of all information assets, including information systems, information system components, software, and information repositories (both electronic and paper). The inventory shall contain a listing of all programs and information systems identified as processing, storing, or transmitting California Department of Corrections and Rehabilitation (CDCR), California Correctional Health Care Services (CCHCS), and California Prison Industry Authority (CALPIA), hereinafter referred to as department, information.

(2) The department uses computer software applications that are owned by the state, as well as commercial software and open-source software (OSS) licensed for use from vendors.

(3) This policy identifies department requirements for the management of department software assets.

(b) Objectives

The objective of this policy is to establish formalized control and management of all types of software including the development of requisite tools, processes procedures and standards.

(c) Scope and Applicability

(1) The scope of this policy extends to all state and agency software assets owned or licensed by the department.

(2) This policy applies to the department Information Security Officer, Program Management, Owners of Information Assets, and Information Asset Custodians.

(d) Policy Directives

The department shall:

(1) Maintain a detailed inventory of all approved department state-owned, commercial and open-source software, including licensing requirement(s), currency, and the cost of the software.

(2) Control and manage all instances and usage of approved department software installed on department information assets in order to comply with all applicable legal, copyright, and licensing requirements.

(3) Establish a continuous monitoring process to identify, detect, and remove all unapproved department software installed or operating on department information assets.

(4) Develop, implement, and maintain a software management plan.

(5) Identify and track any department software that is at end-of-support /end-of-life, and shall ensure that maintenance agreements and processes are in place where appropriate to ensure software can remain operational to meet business requirements.

(6) Establish and maintain controls to prevent unauthorized personnel from installing software applications on state information assets.

(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 and provide advice in the evaluation and selection of department software.

(B) The ISO shall assist and provide advice in the identification of security requirements that software shall comply with.

(3) Department Owners of Information Assets and Program Management

(A) Owners of Information Assets shall ensure that this policy is implemented and shall review the policy's implementation annually.

(B) Owners of Information Assets shall ensure that software assets under their purview are controlled and managed.

(4) Department Information Asset Custodians

(A) Information Asset Custodians shall implement software management, licensing, and usage controls as approved by Owners of Information Assets.

(B) Information Asset Custodians shall maintain all department software licenses associated with commercial products on behalf of Owners of Information Assets.

(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
- Statewide Information Management Manual 120, Software Management Plan Guidelines
- State Administrative Manual, Section 5305.5, Information Asset Management
- State Administrative Manual, Section 5315.7, Software Usage Restrictions
- State Administrative Manual, Section 4846.1, Software Management Plan
- State Administrative Manual, Section 4846.2, Software Management Policy Reporting Requirements
- National Institute of Standards and Technology, Special Publications 800-53, Configuration Management, CM-8, CM-10, CM-11
- National Institute of Standards and Technology, Special Publications 800-53, System and Information Integrity, SI-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 46030.4
- California Government Code Section 11549.3

Revision History

Effective: 11/30/2022