5.3.11 Endpoint Security

(a) Introduction and Overview

(1) Department information assets are often used to conduct business functions internally as well as with other State and non-department persons and devices on the Internet. Devices used for such department business purposes are comprised of servers, network devices, and end user devices including mobile computers, tablets, and smart phones; such devices are collectively called "endpoints" or "endpoint devices." Some department information assets are more prone to loss or theft due to their size, mobility, or location of use.

(2) The department needs to ensure that endpoints are suitably protected to prevent unauthorized access to data and information that may reside on the endpoints.

(b) Objectives

Objectives for this policy are to define the requirements to protect department endpoints that may routinely interact with unknown or untrusted devices on the Internet, or that are more susceptible to loss or theft.

(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 ensure that:

(1) All department endpoints are identified and endpoint asset inventories are documented and continually updated.

(2) Risks to individual department endpoint device types and the data they access, process, and store are assessed.

(3) The requisite endpoint protection controls, as referenced in the Statewide Information Management Manual, are implemented and maintained to mitigate risks to each endpoint.

(4) Endpoint protection controls include people (asset users), processes, and technology controls.

(5) Endpoint protection controls are continuously monitored.

(6) Endpoint protection controls are reviewed at least annually.

(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 with the identification and selection of endpoint protection controls.

(B) Shall ensure that endpoint protection controls meet department requirements for security and privacy.

(3) Department Owners of Information Assets and Program Management:

(A) In collaboration with the Information Asset Custodians shall ensure that the endpoint protection controls are defined, documented, and implemented, and that implementation is reviewed annually.

(B) In collaboration with the Information Asset Custodians shall ensure the endpoint protection controls commensurate with the sensitivity or criticality of the asset are implemented for assets under their purview.

(4) Department Information Asset Custodians:

(A) Shall implement the requisite endpoint protection controls based upon the sensitivity or criticality of the assets as defined by the Owners of Information Assets.

(B) Shall maintain and update endpoint protection technologies based on best practices.

(C) Shall maintain records of endpoint protection controls and ensure proper change management.

(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, 5305-A, Information Security Program Management Standard
- Statewide Information Management Manual, 5355-A, Endpoint Protection Standard
- State Administrative Manual, Section 5355, Endpoint Defense
- State Administrative Manual, Section 5355.1, Malicious Code Protection
- National Institute of Standards and Technology, Special Publications 800-53, Security Assessment and Authorization, CA-7
- National Institute of Standards and Technology, Special Publications 800-53, Configuration Management, CM-2, CM-3, CM-6, CM-7, CM-10, CM-11
- National Institute of Standards and Technology, Special Publications 800-53, System and Communications Protection, SC-8, SC-10, SC-11, SC-13, SC-18, SC-23, SC-24, SC-28, SC-38, SC-42, SC-43
- National Institute of Standards and Technology, Special Publications 800-53, System and Information Integrity, SI-2, SI-3, SI-4, SI-5, SI-7, SI-8, SI 11
- National Institute of Standards and Technology, Special Publications 800-53, Program Management, PM-9
- National Institute of Standards and Technology, Special Publications 800-53, Risk Assessment, RA-2, RA-3, RA-5
- National Institute of Standards and Technology, Special Publications 800-53, Physical and Environmental Protection, PE-3, PE-19, PE-20
- 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 Government Code, Section 11549.3

Revision History

Effective: 02/2022