5.3.19 Audit and Accountability

(a) Introduction and Overview

(1) In order to detect and respond to signs of attack, anomalies, and suspicious or inappropriate activities, California Department of Corrections and Rehabilitation (CDCR), California Correctional Health Care Services (CCHCS), and California Prison Industry Authority (CALPIA), hereinafter referred to as department, requires an audit and security event logging strategy to continuously monitor access and activities conducted using department information assets.

(2) Information assets owned by the department are strategic assets intended for official business use, and are entrusted to state personnel and business partners in the performance of their job-related duties. Since inappropriate or unauthorized access and use of department information assets could result in harm to the state and to the department, it is important to detect and respond to signs of attack, anomalies, and suspicious or inappropriate activities in a timely and proper manner.

(b) Objectives

This policy guides the development and implementation of department event logging and continuous monitoring strategy and supporting processes to identify and respond to indicators of attack, anomalies, and suspicious or inappropriate activities.

(c) Scope and Applicability

(1) The scope of this policy extends to all information assets owned or operated by the department.

(2) This policy is applicable to department Owners of Information Assets and Information Asset Custodians.

(d) Policy Directives

Department Owners of Information Assets in collaboration with Information Asset Custodians and the department Information Security Officer (ISO) shall develop and implement an event logging and continuous monitoring strategy of access and activities conducted using department information assets. This strategy shall include, at a minimum, the following items:

(1) Define and document the audit logging requirements and security events that shall be recorded, monitored, and reviewed.

(2) Identify and implement controls for audit trails and auditability of events for each system as well as for the internal network, accounting for segregation of duties, as appropriate.

(3) Perform, at minimum, monthly monitoring of event logs of critical information assets to identify and respond to indicators of attacks, anomalies, and suspicious or inappropriate activities in a timely manner.

(4) Define secure storage and retention of event logs.

(5) Clearly define roles and responsibilities for event logging and monitoring.

(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 (2) years.

(2) Department Information Security Officer (ISO)

The ISO shall guide the development and implementation of the department event logging and continuous monitoring strategy.

(3) Department Owners of Information Assets and Program Management

(A) Owners of Information Assets in collaboration with Information Asset Custodians are responsible for ensuring the protection of information assets under their purview.

(B) Owners of Information Assets shall participate in the development and implementation of an event logging and continuous monitoring strategy.

(C) Owners of Information Assets shall ensure assets are independently and continuously monitored based on the criticality of information assets.

(4) Department Information Asset Custodians

(A) Information Asset Custodians shall participate in the development and implementation of an event logging and continuous monitoring strategy.

(B) Information Asset Custodians shall implement and maintain the department event logging and continuous monitoring strategy.

(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 5340-A, Incident Reporting and Response Instructions
- State Administrative Manual, Section 5335, Information Security Monitoring
- State Administrative Manual, Section 5335.1, Continuous Monitoring
- State Administrative Manual, Section 5335.2, Auditable Events
- National Institute of Standards and Technology Special Publications 800-53, Audit and Accountability, AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-10, AU-11
- National Institute of Standards and Technology Special Publications 800-53, Physical and Environmental Protection, PE-2, PE-6, PE-8
- National Institute of Standards and Technology Special Publications 800-53, Risk Assessment, RA-3
- California Department of Corrections and Rehabilitation, Department Operations Manual, Chapter 3, Article 22
- California Government Code Section 11549.3

Revision History

Effective: 11/30/2022