5.3.24 Incident Response

(a) Introduction and Overview

(1) California Department of Corrections and Rehabilitation (CDCR), California Correctional Health Care Services (CCHCS), and California Prison Industry Authority (CALPIA), hereinafter referred to as department, management shall promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. Incidents could also include unauthorized access of information asset and incidents negatively affecting the operation, confidentiality, integrity, or availability of information assets. All entities are required to report information security incidents in accordance with the state information security notification and reporting requirements.

(2) Effective incident management includes the formulation, adoption, and maintenance of a written incident management plan that provides for the timely assembly of appropriate staff that are capable of developing a response to, appropriate reporting about, and successful recovery from a variety of incidents. A defined and documented security incident response plan shall enable the department to detect, respond, and recover from security incidents in a timely and organized manner so as to minimize the impacts of the security incident.

(b) Objectives

The objective for this policy is to establish the requirements for a department security incident response plan.

(c) Scope and Applicability

(1) The scope of this policy extends to all state and agency information assets owned or operated by the department as well as information assets managed by third parties on behalf of the department.

(2) This policy applies to all department personnel.

(d) Policy Directives

The department shall:

(1) Ensure that a security incident response plan and related procedures, including specific responses to incidents involving Personally Identifiable Information (PII) are defined, documented and implemented.

(2) Ensure that the security incident response plan and procedures clearly define and document roles and responsibilities to address the full incident life cycle, including:

(A) Security incident detection and identification

(B) Security incident response management

(C) Incident handling team(s), with broad participation from other department stakeholders, under the coordination of a designated incident manager.

(D) Preservation of evidence, including tracking and maintaining the evidence pertaining to chains of custody and evidence.

(3) Ensure that mechanisms and procedures are implemented to enable personnel to report security incidents to the appropriate security staff and the department's Office of Information Security. Ensure all department personnel are aware of incident reporting mechanisms and procedures.

(4) Immediately report incidents through the California Compliance and Security Incident Reporting System (Cal-CSIRS) providing the incidents meet the reporting requirements. Cal-CSIRS requires specific details about the incident and shall notify the California Department of Technology Office of Information Security (OIS), as well as the California Highway Patrol (CHP) Computer Crimes Investigation Unit.

(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 shall ensure that the department has a formally documented and operational incident response plan to address incidents involving the loss, damage, misuse or unauthorized access of information assets, and breaches of security involving personal information in any form, in the most expedient and effective manner.

(C) The CIO or designee shall ensure that the security incident response plan and procedures describe the necessary roles and responsibilities, and activities to enable security incident handlers to effectively prepare for, detect, analyze, contain, eradicate and recover from security incidents.

(D) The CIO or designee shall ensure that security incident response management is integrated across the department, and with other state and department contingency and emergency management plans, teams and advisory resources.
(E) The CIO or designee shall ensure that all department personnel receive incident response and awareness training and education in accordance with the individual's functional role within the department.
(F) The CIO or designee shall ensure that department incident response capabilities are exercised at least annually to test incident response effectiveness, and that results from tests are documented and reviewed to continuously improve capabilities.
(G) The CIO or designee shall ensure that post-mortem/lessons-learned sessions following security incident response activities and tests are completed in order to continually improve incident response capabilities.
(H) The CIO or designee shall ensure that all security incidents and department responses are monitored and documented, and all related activities and decisions are recorded.
(I) The CIO or designee shall ensure that the department incident response plan, procedures and supporting documentation are updated at minimum on an annual basis.
(J) The CIO or designee is responsible for ensuring that this policy is reviewed annually and updated accordingly.
(K) 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 Owners of Information Assets and Information Asset Custodians in the development of department incident response plans.
(B) The ISO shall participate in incident response and management activities.

(3) Department Owners of Information Assets and Program Management.
Owners of Information Assets shall participate and provide assistance with and decisions related to responding to incidents involving information assets under their purview, as required, and as requested by incident managers, the Chief Information Officer (CIO) or Designee and the department ISO.

(4) Department Information Asset Custodians
(A) Information Asset Custodians shall participate and provide assistance with incident response activities as directed and guided by incident managers, ISOs, and Owners of Information Assets, as appropriate.
(B) Information Asset Custodians shall maintain records related to and supporting individual incident responses.

(5) Department Users
(A) Users shall be aware of and adhere to all department information security and privacy policies.
(B) Users shall report any incidents of possible misuse or violation of this policy to the department ISO, designee, or appropriate security staff or their immediate supervisor.

(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 5340-A, Incident Reporting and Response Instructions
- Statewide Information Management Manual 5340-B, Information Security Incident Report (Cal-CSIRS)
- Statewide Information Management Manual 5340-C, Requirements to Respond to Incidents Involving a Breach of Personal Information
- State Administrative Manual, Section 5340, Information Security Incident Management
- State Administrative Manual, Section 5340.1, Incident Response Training
- State Administrative Manual, Section 5340.2, Incident Response Testing
- State Administrative Manual, Section 5340.3, Incident Handling
- State Administrative Manual, Section 5340.4, Incident Reporting
- National Institute of Standards and Technology, Special Publications 800-53, Contingency Planning, CP-2, CP-9, CP-10, CP-13
- 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, IR-8, IR 9, IR-10
- 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
- National Institute of Standards and Technology, Special Publications 800-53, Security Assessment and Authorization, CA-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, 49020.12, 49020.12.1, 49020.12.2
- California Government Code Section 11549.3

Revision History
Effective: 11/30/2022