5.3.23 Identification and Authentication

(a) Introduction and Overview

Information assets owned by California Department of Corrections and Rehabilitation (CDCR), California Correctional Health Care Services (CCHCS), and California Prison Industry Authority (CALPIA), hereinafter referred to as department, are intended to be accessed by authorized entities and used exclusively for department business purposes. Consequently, it is imperative that all entities requesting access to department information assets are uniquely identified prior to being granted access.

(b) Objectives

The objective for this policy is to establish department requirements to control access to information assets by uniquely identifying the entities requesting access before access is granted.

(c) Scope and Applicability

(1) The scope of this policy extends to all state and agency 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 all department personnel and processes acting on behalf of the department.
(3) This policy governs physical and logical access. Logical access includes local access and network, including remote access.

(d) Policy Directives

(1) The department shall ensure that a department identity and access management (IAM) strategy is developed, clearly defined, documented, and implemented.
(2) The department IAM strategy shall include the following:
(A) Requirements to meet all state and federal requirements.
(B) The unique identification of all authorized personnel or processes acting on behalf of the department that access department information assets prior to being granted access.
(C) The use of appropriate credentials for the identification of non-state personnel.
(D) Implement methods that enable non-repudiation of access requests to information assets containing sensitive and confidential data, and protect related audit logs for a period of no less than six months.
(E) Implementation of a suitable IAM infrastructure supporting department requirements.
(F) Implementation of safeguards to protect the confidentiality, integrity, and availability of the supporting IAM infrastructure.
(G) Definition and implementation of authentication mechanisms based on the type and method of access and the inherent risks associated with each access use case.
(H) Control and management of access by administrative and privileged users, including the ability to immediately revoke access when necessary.
(I) Requirement to implement application level identification and authentication in addition to platform level access to provide additional security, as appropriate by Owners of Information Assets.
(J) Definition, documentation, and implementation of audit and security activity and event logging requirements for privileged use.
(K) Identification, development, and implementation of supporting identity and access management processes and procedures.

(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 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 in collaboration with Information Asset Custodians shall ensure that identification and authentication technologies and process controls commensurate with the sensitivity or criticality of the asset are implemented for assets under their purview.

(3) Department Information Asset Custodians
(A) Information Asset Custodians shall assist Owners of Information Assets in selecting and implementing identification and authentication technologies and process controls commensurate with the sensitivity or criticality of the asset.
(B) Information Asset Custodians shall maintain the identification and authentication infrastructure and supporting processes and procedures.
(C) Information Asset Custodians shall maintain identification and authentication records as defined by Owners of Information Assets for a minimum of twelve (12) months, or as defined by the department's Information Security Officer (ISO).
(4) Department Users
(A) Users shall report any incidents of possible misuse or violation of this policy to the department ISO, designee, appropriate security staff or their immediate supervisor.
(B) Users shall be aware of and adhere to all department information security and privacy policies.

(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 5360-A, Telework and Remote Access Security Standard
- State Administrative Manual, Section 5335, Information Security Monitoring
- State Administrative Manual, Section 5340, Information Security Incident Management
- State Administrative Manual, Section 5360, Identity and Access Management
- National Institute of Standards and Technology, Special Publications 800-53, Identification and Authentication, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA 7, IA-8, IA-9, IA-10, IA-11, IA-12

- National Institute of Standards and Technology, Special Publications 800-53, Access Control, AC-1, AC-2, AC-3, AC-4, AC-5, AC-5, AC-7, AC-8, AC 9, AC-10, AC-11, AC-12, AC-13, AC-14, AC-15, AC-16, AC-17, AC-18, AC-19, AC 20, AC-21, AC-22, AC-23, AC-24, AC-25
- National Institute of Standards and Technology, Special Publications 800-53, Audit and Accountability, AU-1, AU-2, AU-10, AU-11, AU-12, AU-13
- 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, Sections 49020.5, 49020.10
- California Government Code Section 11549.3

Revision History
Effective: 11/30/2022