5.3.14 Access Control

(a) Introduction and Overview

(1) Information assets owned by the California Department of Corrections and Rehabilitation (CDCR), California Correctional Health Care Services (CCHCS), and California Prison Industry Authority (CALPIA) 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.

(2) Access may enable or restrict the ability to do something with a resource. Access control, then, is the selective restriction of these abilities and is comprised of both physical and logical access.

(b) Objectives

Objectives for this policy are to:

(1) Enable the development and implementation of a CDCR, CCHCS, and CALPIA (hereinafter referred to as department) identity and access management strategy that comprehensively addresses all access to department information assets.

(2) Document requirements for the appropriate control and management of physical and logical access to, and the use of department information assets.

(3) Require the use of appropriate authentication methods based on the type and sensitivity of information assets being accessed.

(4) Govern the use of privileged access rights, such as those assigned to Administrator and Privileged Accounts.

(c) Scope and Applicability

This policy applies to all personnel; all information assets owned or operated by the department; and all forms of physical and logical access to department information assets, including using wired, wireless, and remote access network connections. All department personnel shall comply with this policy.

(d) Policy Directives

(1) Before department Information Technology infrastructure network access, users shall be identified and authenticated.

(2) Users accessing sensitive or confidential information shall be appropriately provisioned before accessing department owned or operated information assets and associated facilities.

(A) In the case of physical access to facilities, where access control is a manual process, authentication shall be accomplished by manual verification of an identity (e.g., photo ID).

(3) Access to department information assets and associated permissions shall be approved by the respective department information asset owner.

(4) Records of all user account creations, deletions, and changes to user access and permissions shall be maintained for a period of at least 12 months.

(5) The department shall develop a comprehensive identity and access management strategy based on statutory and organizational business requirements, including:

(A) Supporting unique identification, individual user types and groups, job roles and access methods.

(B) Limiting access to information assets and associated facilities to authorized users, processes, or devices, and to authorized activities and transactions.

(C) Defining roles and assigning responsibilities pertaining to access control tools, technologies and processes.

(D) Developing and implementing standards, technologies and processes to support its access control strategy.

(E) Formally defining and documenting user account types and groups, and access use cases, commensurate with employment responsibilities.

(F) Employing multi-factor authentication for remote access, and risk-based user authentication methods to accommodate approved logical access use cases.

(G) Publicly available or published access and authentication credentials, such as default credentials, anonymous credentials and guest credentials, shall not be re used, and shall be replaced as a matter of standard procedure.

(H) Display a notification of system use or security warning banner message on each system that requires affirmative acknowledgement by the user before authentication.

(6) The department shall ensure that access to non-active personnel is deactivated before or immediately after termination, as appropriate.

(7) The department shall review and validate user access and associated access permissions and privileges at least every 12 months to ensure alignment with individual job roles and functions.

(8) Certain department information technology support personnel and network administrators shall require specific privileges to perform their duties.
  (A) For all Administrators and Privileged Account holders, the department shall:
    1. Identify and document all Administrator and Privileged Account holders.
    2. Ensure that administrative and privileged accesses are granted to users through established or approved local provisioning processes.
    3. Ensure that such users acknowledge the privileges and only use those accounts to fulfill the specific job responsibilities for which the privileges apply.
    4. Ensure automated processes including service accounts with privileged access to information systems shall follow established standards for password rotation, limited access and auditing.
    5. Review and validate the continued business need for all Administrator and Privileged Accounts on an annual basis or when staffing, resource, or job function changes occur.

(9) User access and permissions shall be based on the principles of least privilege and separation of duties.

(10) The department shall define and document all auditable system events related to data and information access that shall be recorded.

(11) The department shall ensure access control management systems are configured to capture and record audit and security information related to access events.

(12) Audit and security records shall be securely stored and protected against tampering; audit and security records shall be maintained for the period defined in the records retention schedule.

(13) Monitoring and alerting of anomalous or suspicious activities and events is most effectively accomplished through automated and real-time reviews of audit and security logs.

(14) The department shall implement suitable controls to monitor for unauthorized changes to user access. Where feasible, unauthorized changes shall generate automated alerts to notify responsible department individuals.

(15) In the absence of automated monitoring and alerting, the department Information Security Officer (ISO) shall review access record reports on a quarterly basis. Access records include: new user account creation requests, user access revocation requests, active user lists, and user termination lists.

(e) Roles and Responsibilities

(1) The department Chief Information Officer (CIO) or Designee:
  (A) 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) 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 two years.

(2) Department Owners of Information Assets and Program Management:
  (A) In collaboration with the Information Asset Custodians shall ensure that this policy is implemented and implementation is reviewed at minimum annually.
  (B) Shall audit and assess user access rights and privileges to ensure alignment with individual job roles and functions on an annual basis.

(3) Department Information Asset Custodians:
  (A) Shall implement user access and associated rights and privileges as requested and approved by Owners of Information Assets.
  (B) In collaboration with Owners of Information Assets, shall periodically review accounts with elevated privileges and verify that continued privilege account access is required.
  (C) In collaboration with Owners of Information Assets shall ensure access technology and process controls are commensurate with the sensitivity or criticality of information assets under their purview.
  (D) Shall revoke or modify individual user access rights and privileges upon notification from the Owners of Information Assets.
  (E) Shall maintain access records consistent with the retention schedule.

(f) Enforcement

(1) Non-compliance with this policy may result in disciplinary or adverse action as set forth in 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 is technically impossible, if existing policy currently in place already meets these requirements, or if deviation from this policy is necessary to support a business function, the respective manager shall formally request a security variation as defined by the department ISO.

(j) Authority

This policy complies with 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, Section 5305-A, Information Security Program Management Standard
- State Administrative Manual, Section 5305.4, Personnel Management
- State Administrative Manual, Section 5305.7, Risk Assessment
- State Administrative Manual, Section 5315, Information Security Integration
- State Administrative Manual, Section 5335, Information Security Monitoring
- State Administrative Manual, Section 5335.1, Continuous Monitoring
- State Administrative Manual, Section 5335.2, Auditable Events
- State Administrative Manual, Section 5355, Endpoint Defense
- State Administrative Manual, Section 5355.1, Malicious Code Protection
- State Administrative Manual, Section 5360, Identity And Access Management
- State Administrative Manual, Section 5360.1, Remote Access
- State Administrative Manual, Section 5360.2, Wireless Access
- State Administrative Manual, Section 5365.1, Access Control for Output Devices
- National Institute of Standards and Technology, Special Publications 800-53, Access Control, AC-1, AC-2 (1)(2)(3)(4), AC-3, AC-4, AC-5, AC-6 (1)(2)(5)(9)(10), AC-7, AC-8, AC-11, AC-12, AC-14, AC-17(1)(2)(3)(4), AC-18(1), AC 19(5), AC-20(1)(2), AC-21, AC-22, AC-24
- National Institute of Standards and Technology, Special Publications 800-53, Audit & Accountability, AU-3, AU-6, AU-7, AU-8, AU-9, AU-10, AU 11, AU-13
- National Institute of Standards and Technology, Special Publications 800-53, Awareness & Training, AT-2
- National Institute of Standards and Technology, Special Publications 800-53, Identification & Authorization, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA 8, IA-9, IA-10, IA-11
- National Institute of Standards and Technology, Special Publications 800-53, Risk Assessment RA-1, RA-2, RA-3
- 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 49020.6.1, 49020.7.1, 49020.9, 49020.10
- California Government Code, Section 11549.3

Revision History
Effective: 03/2022