5.3.13 Server Configuration

(a) Introduction and Overview

This document defines the policy for all servers, physical and virtual, owned or operated by the department. Effective implementation of this policy minimizes the risk of server vulnerabilities that can result in system unavailability, data corruption, unauthorized access, information and resource misuse, and service disruption.

(b) Objectives

The objective of this policy is to establish the base configuration of internal server equipment that is owned and operated by the department. Effective implementation of this policy will minimize unauthorized access to department proprietary information and technology.

(c) Scope and Applicability

(1) The scope of this policy extends to all information assets owned or operated by the department, including critical infrastructure, as well as information assets owned or operated by third-parties on behalf of the department.

(2) This policy applies to Owners of Information Assets and Information Asset Custodians.

(d) Policy Directives

(1) The department shall:

(A) Only create server service accounts when necessary.

(B) Use the Principle of Least Privileged to limit user access rights to a minimum.

(C) Not use administrative accounts (e.g., root, administrator, O365 Global) when a non-privileged account will suffice.

(D) Disable/lock/delete all accounts except those required to provide necessary services.

(E) Change the default passwords for all accounts and follow password security best practices outlined in Statewide Information Management Manual (SIMM) 5300-A, Org-Defined Standards, (National Institute of Standards and Technology [NIST] IA-5(1)).

(F) Limit access to administrative accounts to only those who have operational need and have been authorized.

(G) Ensure service accounts are not part of Local Administrators or Domain Administrator accounts.

(H) Authorize and document all administrative (privileged) accounts.

(I) Encrypt all passwords and all sensitive and confidential data while in transit. Passwords shall adhere to State Org-Defined Policy. (See State Administrative Manual [SAM] 5350.1, SIMM 5300-B and NIST, Special Publications [SP] 800-63B, FIPS 140-2).

(J) Authenticate users over encrypted protocols.

(K) Log all access to the server and services that are protected through access control methods.

(L) Establish and implement controls to ensure that service account functions are authorized using service account credentials only.

(2) Systems Configuration and Maintenance

(A) Servers shall be patched and hardened before attaching them to the network. Security patches shall be installed on the system not less than monthly. If an intelligence source advises of an imminent threat, patches shall be installed according to documented information technology standards.

(B) Servers shall be physically secured in locations accessible only to authorized personnel.

(C) Only required services shall be enabled or installed on the server. Services that are not required shall be uninstalled or disabled.

(D) Regular back-ups of the server shall be completed according to the back-up and retention policy and tested on a periodic schedule.

(3) Monitoring

(A) The server shall capture and archive critical user, network, system, and security event logs to enable review of system data for forensic and recovery purposes.

(B) Security-related events shall be reviewed and investigated. Events include, but are not limited to:

1. Account lockouts
2. Failed user account logins
3. Evidence of unauthorized access to privileged accounts
4. Anomalous occurrences that are not related to specific applications on the server

(C) Security incidents shall be handled immediately in accordance with SAM and SIMM and reported to the department Information Security Officer (ISO), the data owners or their designees.

(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 ISO:
  (A) Shall assist Owners of Information Assets and information asset custodians in the identification of data security controls and processes.
  (B) Shall ensure data security controls, methods, and processes meet department and applicable regulatory requirements for security.
  (C) Shall participate in all incidents involving information security.

(3) 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 annually and as appropriate.
  (B) Shall audit user access rights and privileges to ensure alignment with individual job roles and functions on an annual or more frequent basis as appropriate.

(4) Department Information Asset Custodians:
  (A) Shall review accounts with privileged access no less than semi-annually and verify that continued privileged access is required.
  (B) In collaboration with Owners of Information Assets, shall ensure the information security control measures are commensurate with the sensitivity or criticality of information assets under their purview.
  (C) Shall assist Owners of Information Assets in identifying data security controls commensurate with the classification of the data.
  (D) Shall document, implement, monitor, and maintain data security protection controls based upon the sensitivity or criticality of the assets.
  (E) Shall develop and implement tools, technologies, processes, and procedures to support, monitor, and maintain data security controls.
  (F) Shall maintain data security records.

(f) Enforcement

(1) Non-compliance with this policy may result in disciplinary or adverse action as set forth in the California Deparmtent 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, Section 5300-B, Foundational Framework
- Statewide Information Management Manual, Section 5305-A, Information Security Program Management Standard
- State Administrative Manual, Section 5305.5, Information Asset Management
- State Administrative Manual, Section 5310.4, Individual Access to Personal Information
- State Administrative Manual, Section 5310.6, Data Retention and Destruction
- State Administrative Manual, Section 5310.7, Security Safeguards
- 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
- State Administrative Manual, Section 5350.1, Encryption
- State Administrative Manual, Section 5365, Physical Security
- State Administrative Manual, Section 5365.1, Access Control for Output Devices
- State Administrative Manual, Section 5365.2, Media Protection
- State Administrative Manual, Section 5365.3, Media Disposal
- Federal Information Processing Standards, FIPS 199
- Federal Information Processing Standards, FIPS 140-2
- National Institute of Standards and Technology, Special Publications 800-53, Access Control, AC-3, AC-4
- National Institute of Standards and Technology, Special Publications 800-53, Audit and Accountability, AU-2, AU-3, AU-13
- National Institute of Standards and Technology, Special Publications 800-53, Configuration Management, CM-8
- National Institute of Standards and Technology, Special Publications 800-53, Identification and Authentication, IA-5(1)
- National Institute of Standards and Technology, Special Publications 800-53, Media Protection, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7
- National Institute of Standards and Technology, Special Publications 800-53, Physical and Environmental Protection, PE-5, PE-19, PE-20
- National Institute of Standards and Technology, Special Publications 800-53, Planning, PL-4
- 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 and Communications Protection, SC-4, SC-8, SC-13, SC-17, SC-28
- National Institute of Standards and Technology, Special Publications 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management
- 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