5.3.16 Firewall Configuration

(a) Introduction and Overview

Network firewalls act as a communications buffer between internal and external devices while simultaneously keeping out unwanted users, viruses, worms, or other malicious programs trying to access the protected network. Firewalls and the technology and procedures that support them help protect internal networks and manage traffic in and out of California Department of Corrections and Rehabilitation (CDCR), California Correctional Health Care Services (CCHCS), and California Prison Industry Authority (CALPIA)'s network.

(b) Objectives

The objective of this policy is to define how firewalls are to be configured, implemented, and managed within the CDCR, CCHCS, and CALPIA (hereinafter referred to as department).

(c) Scope and Applicability

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

(2) This policy applies to the department Chief Information Officer or their designee, Information Technology functions, information security sections, owners of critical infrastructure, Agency and Department Information Security Officers, Technology Recovery Plan coordinators, and Information Asset Custodians.

(d) Policy Directives

(1) The department shall use a multi-layered approach to protect computer resources and assets. Network security design shall include firewall functionality at all places in the network where opportunities exist for outside exploitation. This may include placing a firewall in areas other than the network perimeter to provide an additional layer of security and protect devices that are placed directly onto external networks (i.e. the Demilitarized Zone [DMZ]) or between different trusted and untrusted segments of the network.

(2) Firewall Configuration

The department shall:

(A) Implement configurations that restrict all inbound and outbound traffic associated with untrusted wired/wireless networks and hosts.

(B) Deny all traffic by default and only allow inbound and outbound traffic thru approved exceptions.

(C) Disable unnecessary user accounts and default accounts (e.g. Administrator, Guest, etc.).

(D) Disable all unused and unnecessary ports, protocols, and services before deployment into a production environment.

(E) Implement a DMZ that limits inbound traffic to the internal trusted network and permits authorized publicly accessible services, protocols, and ports/services.

(F) Log all changes to firewall configuration parameters, enabled services, and permitted connectivity paths for a period of one year. The department data retention procedures shall be followed.

(G) Physically secure firewalls in a location accessible only to authorized personnel. The placement of firewalls in an open area within a general-purpose data center is prohibited.

(e) Firewall Administration and Management

The following firewall management practices shall be utilized:

(1) Configuration of rulesets and policies shall be managed through an internal change management process.

(2) Firewall security logs shall be reviewed no less than every six months to detect any unauthorized entry attempts or network anomalies, and shall be retained for a period of one year.

(3) All enterprise firewall rulesets shall be reviewed according to documented processes and procedures.

(4) All new inbound and outbound connections requiring firewall rulesets to be applied shall have a valid business justification and the approval of the Information Asset Custodian on behalf of the Information Asset Owner.

(5) Current security updates, patches, and anti-virus definitions shall be applied in accordance with documented standards, threat intelligence, and product/vendor guidance.

(6) Administrative access shall be restricted to authorized and approved Information Asset Custodians and designated security personnel.

(7) Access to management and administrative interfaces shall be available only from locations that are deemed appropriate.

(f) 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) The department Information Security Officer (ISO) is responsible for the oversight and coordination of entity information security policies and procedures.

(3) The department Owners of Information Assets and Program Management, in collaboration with the Information Asset Custodians, are responsible for ensuring the protection of information assets under their purview.

(4) The department Information Asset Custodians:
  (A) In collaboration with the Information Asset Owners, are responsible for ensuring implementation of this policy and its directives.
  (B) Shall review firewall security logs in accordance with this policy.
  (C) Shall notify the department ISO and the asset owner shall a security incident occur.

(5) The department Firewall Administrators are responsible for managing firewall policies, updates, upgrades, software, installations, as well as other network security solutions. As access and network requirements change, firewall policies shall be updated to reflect these changes.

(g) 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.

(h) 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.

(i) Reporting

Violations of this policy shall be reported to the department ISO.

(j) 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 department ISO.

(k) Authority

This policy complies with State of California Government Code Section 11549.3 and State Administrative Manual-5350 Operational Security.

(l) Revisions

The CIO or designee shall ensure that the contents of this article are current and accurate.

References

- 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 Standard, FIPS 199
- National Institute of Standards and Technology, Special Publications 800-53, Access Control, AC-3 Access Enforcement, AC-4 Information Flow Enforcement
- National Institute of Standards and Technology, Special Publications 800-53, Audit and Accountability, AU-2 Event Logging, AU-3 Content of Audit Records, AU-13 Monitoring for Information Disclosure
- National Institute of Standards and Technology, Special Publications 800-53, Configuration Management, CM-8 System Component Inventory
- 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 Access Control for Output Devices, PE-19 Information Leakage, PE-20 Asset Monitoring and Tracking
- National Institute of Standards and Technology, Special Publications 800-53, Planning, PL-4 Rules of Behavior
- National Institute of Standards and Technology, Special Publications 800-53, Program Management, PM-9 Risk Management Strategy
- National Institute of Standards and Technology, Special Publications 800-53, Risk Assessment, RA-2 Security Categorization, RA-3 Risk Assessment
- National Institute of Standards and Technology, Special Publications 800-53, Assessment, Authorization and Monitoring, CA-7 Continuous Monitoring
- National Institute of Standards and Technology, Special Publications 800-53, System and Communications Protection, SC-4 Information in Shared Resources, SC-8 Transmission Confidentiality and Integrity, SC-13 Cryptographic Protection, SC-17 Public Key Infrastructure Certificates, SC-28 Protection of Information at Rest
- 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 49020.8, 49020.9 and 49020.10
- California Government Code, Section 11549.3

Revision History
Effective: 03/2022