# System and Communication Protection Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives.*

### **S**ecurity boundary under scope

1. [List of applicable systems]

### References

1. NIST 800-160:<https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final>
2. NIST SP 800-207:<https://csrc.nist.gov/pubs/sp/800/207/final>
3. NIST SP 800-215:<https://csrc.nist.gov/pubs/sp/800/215/final>
4. NIST SP 800-153:<https://csrc.nist.gov/pubs/sp/800/153/final>
5. NIST 800-175A:<https://csrc.nist.gov/pubs/sp/800/175/a/final>
6. NIST 800-175B:<https://csrc.nist.gov/pubs/sp/800/175/b/r1/final>
7. NIST FIPS 140-3:<https://csrc.nist.gov/pubs/fips/140-3/final>
8. ISO/IEC 18033:<https://www.iso.org/standard/76156.html>
9. ISO/IEC 20648:<https://www.iso.org/standard/76156.html>
10. ISO/IEC 27033-6:<https://www.iso.org/standard/51585.html>
11. ISO/IEC 27001:2022: A.6.7, A.8.20, A.8.21, A.8.22, A.8.23, A.8.24
12. NIST 800-53 rev. 5: AC-4, AC-17, AC-17(3), AC-18, AC-18(1), AC-19(5), CM-7, CM-7(1), CM-7(2), CM-7(5), CP-9(8), MP-5, PL-8, SA-9(2), SC-2, SC-7, SC-7(3), SC-7(4), SC-7(5), SC-7(7), SC-7(8), SC-17, SC-28, SC-28(1), SC-39
13. CIS v8: 4.2, 12.3, 1.2.5, 1.2.8, 12.2, 12.4, 12.6, 12.7, 13.4, 13.5
14. PCI DSS 4.0: 1.1.1, 1.2.1, 1.2.3, 1.2.4, 1.2.8, 1.3.1, 1.3.2, 1.3.3, 1.4.1, 1.4.2, 1.4.4, 2.3.2, 3.1.1, 3.3.2, 3.3.3, 3.5.1, 3.5.1.1, 3.5.1.2, 3.5.1.3, 4.2.1.2, 8.3.2
15. AICPA SOC 2 TSC: CC2.1, CC6.1, CC6.6, CC6.7, CC8.1, PI1.2, PI1.4, PI1.5

## Document ownership

<(Choose from)>

* 1. Policy Owner:
     1. [Owner name] ([Owner email]), [Owner title]
  2. Information Security Officer:
     1. [Information officer name], ([Information officer email]), [Information officer title]
  3. System Owner(s):
     1. [System owner name], ([System owner email]), [System owner title]
  4. Process and Operational Owner(s)
     1. [process owner], ([process owner email]), [process owner title]
  5. System Administrator(s):
     1. [System admin name], ([System admin email]), [System admin title]
  6. Required Dissemination: <(Choose from)>
     1. IT Administrator
     2. Engineering
     3. Product Management
     4. Support
     5. [responsible party]
     6. [Organization name] Leadership Team
     7. Contractors
     8. Vendors
     9. Company Wide
     10. [Organization name] SIRT
  7. Optional Dissemination: <(Choose from)>
     1. IT Administrator
     2. Engineering
     3. Product Management
     4. Support
     5. [responsible party]
     6. [Organization name] Leadership Team
     7. Contractors
     8. Vendors
     9. Company Wide
     10. [Organization name] SIRT

## Purpose

The purpose of the System and Communication Protection Policy is to establish a framework for securing the organization’s network infrastructure, systems, and communications. This policy aims to protect the integrity, confidentiality, and availability of information by implementing security controls and procedures. It ensures that all network access points, data transmissions, and system functionalities are safeguarded against unauthorized access, disruptions, and other security threats.

## Scope

This policy applies to all employees, contractors, vendors, and any other individuals or entities with access to the organization’s network and information systems. It encompasses the following areas:

* Network access security
* Least functionality of networks and systems
* Network separation and zero trust
* Domain name services protection
* Encryption of data in transit
* Encryption of data at rest
* Session protection
* Domain and security certificate management
* Protection of wireless network traffic
* Traffic filtering
* API security

The policy is applicable to all network devices, servers, databases, applications, communication channels, and any other components that comprise the organization’s information systems infrastructure. This includes, but is not limited to, internal and external networks, cloud services, and third-party services interfacing with the organization’s network.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], **[owner title]** | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | **Executive Team** | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | **Executive Team** | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], **[Information officer title]** | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner],  **Operational owner title]** |  |
| Information Systems Administrators | **System Administrators** | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], **[HR title]** | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users | **End Users** | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | **[provider type]** | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
  2. Management has reviewed and approved this policy.
  3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
  4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties.
  2. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties

## Definitions

* 1. **Access Control List (ACL)**
     1. A set of rules that define permissions and restrictions for accessing network resources.
  2. **Administrative Access**
     1. Privileged access allowing system and network administrators to manage and configure systems and network devices.
  3. **DNS Security Extensions (DNSSEC)**
     1. A suite of specifications to secure information provided by the Domain Name System (DNS) against certain attacks.
  4. **Encryption**
     1. The process of converting data into a coded form to prevent unauthorized access.
  5. **FIPS-Validated Cryptographic Algorithms**
     1. Cryptographic algorithms that have been certified by the Federal Information Processing Standards (FIPS) for use in protecting sensitive data.
  6. **Intrusion Detection and Prevention Systems (IDPS)**
     1. Systems designed to detect and prevent unauthorized access or attacks on network and information systems.
  7. **Network Segmentation**
     1. Dividing a network into smaller parts to improve security and performance by isolating segments to contain and limit potential breaches.
  8. **Public Key Infrastructure (PKI)**
     1. A framework for managing digital certificates and public-key encryption to secure communications.
  9. **Session Hijacking**
     1. An attack where an unauthorized user gains control of a legitimate session between a client and a server.
  10. **Session Timeout**
      1. A security feature that terminates a session after a period of inactivity to prevent unauthorized access.
  11. **SSL/TLS (Secure Sockets Layer/Transport Layer Security)**
      1. Protocols that provide secure communication over a computer network.
  12. **Zero Trust**
      1. A security model that requires all users, whether inside or outside the network, to be authenticated, authorized, and continuously validated before being granted access.
  13. **WPA3 (Wi-Fi Protected Access 3)**
      1. The latest security protocol developed by the Wi-Fi Alliance to secure wireless computer networks.
  14. **Firewall**
      1. A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
  15. **Proxy Server**
      1. A server that acts as an intermediary for requests from clients seeking resources from other servers.
  16. **API (Application Programming Interface)**
      1. A set of rules and tools for building software and applications, enabling different software entities to communicate with each other.
  17. **Authentication**
      1. The process of verifying the identity of a user or system.
  18. **Authorization**
      1. The process of determining if a user or system has permission to access a resource.
  19. **Cryptographic Algorithms**
      1. Mathematical algorithms used for encryption and decryption to secure data.
  20. **Intrusion Prevention System (IPS)**
      1. A network security tool designed to prevent network attacks by identifying and blocking malicious activities in real-time.
  21. **Least Functionality**
      1. A principle of reducing systems and networks to only the essential functions necessary for operation, minimizing potential security vulnerabilities.
  22. **Data at Rest**
      1. Data that is stored physically in any digital form (e.g., databases, data warehouses).
  23. **Data in Transit**
      1. Data actively moving from one location to another, such as across the internet or through a private network.
  24. **Traffic Filtering**
      1. The process of controlling the flow of data packets based on predefined security rules to protect against unauthorized access or attacks.

## Policy

#### Network Access Security

The [responsible party] shall:

* + 1. Implement access control lists (ACLs) on all network devices to restrict unauthorized access.
    2. Ensure secure administrative access to network devices through encryption and management access limited to authorized networks.
    3. Conduct quarterly reviews and updates of network documentation, including network diagrams and configurations.
    4. Employ intrusion detection and prevention systems to monitor and log unauthorized access attempts ​​.

#### Least Functionality of Networks and Systems

The [responsible party] shall:

* + 1. Disable all unused services and ports on network devices and servers.
    2. Remove unnecessary files and services from servers and network devices.
    3. Regularly review system configurations to ensure only essential functionalities are enabled ​​.

#### Network Separation and Zero Trust

The [responsible party] shall:

* + 1. Implement network segmentation to separate publicly accessible systems from internal networks.
    2. Apply zero trust principles, ensuring verification and least-privilege access across all systems and networks.
    3. Continuously monitor and adjust network segmentation based on evolving threats and operational needs ​​.

#### Domain Name Services (DNS) Protection

The [responsible party] shall:

* + 1. Implement DNS Security Extensions (DNSSEC) to provide data origin authentication and integrity verification.
    2. Monitor DNS traffic for signs of malicious activity and unauthorized access attempts.
    3. Regularly update DNS configurations and review access controls​​​​.

#### Encryption of Data in Transit

The [responsible party] and [responsible party] shall:

* + 1. Encrypt all sensitive or confidential data transmitted over public and private networks using FIPS-validated or NSA-approved cryptographic algorithms.
    2. Ensure encryption mechanisms are in place to prevent unauthorized disclosure and detect changes to data during transmission​​​​.

#### Encryption of Data at Rest

The [responsible party] and [responsible party] shall:

* + 1. Encrypt sensitive or confidential data stored on servers, user assets, portable devices, and backup storage.
    2. Monitor data stores and repositories to ensure compliance with encryption policies and procedures.
    3. Use automated tools to detect unencrypted sensitive data and enforce encryption policies​​​​.

#### Session Protection

The [responsible party] shall:

* + 1. Terminate sessions after 10 minutes of inactivity for privileged users and 15 minutes for general users.
    2. Ensure all sessions are encrypted and protected against session hijacking.
    3. Implement session timeout mechanisms to minimize the risk of unauthorized access​​​​.

#### Domain and Security Certificate Management

The [responsible party] shall:

* + 1. Manage and renew all public key infrastructure (PKI) and domain certificates in accordance with organizational policies.
    2. Ensure only approved certificates and trust anchors are included in the organization's certificate stores.
    3. Monitor and audit the usage of security certificates to prevent unauthorized access​​​​.

#### Protection of Wireless Network Traffic

The [responsible party] and [responsible party] shall:

* + 1. Implement strong encryption (e.g., WPA3) for all wireless communications.
    2. Disable wireless networking capabilities when not in use or intended for deployment.
    3. Regularly review and update wireless network configurations to ensure compliance with security policies​​​​.

#### Traffic Filtering

The [responsible party] shall:

* + 1. Employ firewalls and intrusion prevention systems to filter unauthorized traffic and prevent network attacks.
    2. Route all traffic through authenticated proxy servers and monitor for malicious activity.
    3. Implement policies to deny traffic by default and allow by exception at managed network interfaces​​​​.

#### API Security

The [responsible party] shall:

* + 1. Implement authentication and authorization mechanisms for all API endpoints.
    2. Monitor API traffic for anomalies and unauthorized access attempts.
    3. Ensure APIs are securely developed and deployed, following best practices for input validation and data protection​​​​.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
  2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
  3. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
     1. Policies
     2. Procedures
     3. Standards
     4. Documentation
     5. Regulations
     6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
  2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
     1. The Information Security Officer
     2. Officer of the [Organization name] Leadership Team
  3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |