

{Insert Company Name}

Security Policy

System and Communication Protection

**Version:**

{N.N}

**Date:**

{Insert Modified Date}

# Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Any item that needs to be updated within this document can be found with { } around each item and in (RED) Font. [Delete this for final product submission]

# Table of Contents

1 Introduction ............................................................................................................................................. 1

2 Purpose .................................................................................................................................................... 1

3 Scope ........................................................................................................................................................ 2

4 Roles and Responsibilities ........................................................................................................................ 2

5 Management Commitment ..................................................................................................................... 2

6 Authority .................................................................................................................................................. 3

7 Compliance .............................................................................................................................................. 3

8 Policy Requirements ................................................................................................................................ 4

8.1 System and Communications Protection Policies and Procedures [SC-1] ......................................... 4

8.2 Separation of System and User Functionality [SC-2] ......................................................................... 4

8.3 Security Function Isolation [{SC-3 High Only}] ................................................................................... 6

8.4 Information in Shared System Resources [SC-4] ................................................................................ 6

8.5 Denial of Services Protection [SC-5] ................................................................................................... 6

8.6 Boundary Protection [ SC-7, SC-7 (3,4,5,7,8,12,18), {SC-7 (10,20,21) High Only}] ............................. 6

8.7 Transmission Confidentiality and Integrity [SC-8, SC-8 (1)] ............................................................... 7

8.8 Network Disconnect [SC-10] .............................................................................................................. 6

8.9 Cryptographic Key Establishment & Management [SC-12, {SC-12 (1) High Only}] ............................. 6

8.10 Cryptographic Protection [SC-13] ..................................................................................................... 7

8.11 Collaborative Computing Devices and Applications [SC-15] ............................................................ 7

8.12 Public Key Infrastructure Certificates [SC-17] .................................................................................. 7

8.13 Mobile Code [SC-18] ........................................................................................................................ 7

8.14 Secure Name/Address Resolution Service (Authoritative Source) [SC-20] ...................................... 7

8.15 Secure Name/Address Resolution Service (Recursive or Caching Resolver) [SC-21] ....................... 7

8.16 Architecture and Provisioning for Name/Address Resolution Service [SC-22] ................................. 8

8.17 Session Authenticity [SC-23] ............................................................................................................. 8

8.18 Fail in Know State [{SC-24 High Only}] .............................................................................................. 8

8.19 Protection of Information at Rest [SC-28, SC-28 (1)] ........................................................................ 8

8.20 Process Isolation [SC-39] .................................................................................................................. 8

8.21 System Time Synchronization [SC-45, SC-45 (1)] .............................................................................. 9

# Introduction

{Insert Company Name} has developed corporate policies that identify the security requirements for its information systems and personnel in order to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by {Insert Company Name}’s management and in compliance with the Access Control family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.

# Purpose

The purpose of these policies is to establish access control requirements to ensure the confidentiality, integrity, and availability of {Insert Company Name}’s systems, facilities, and data are protected. These policies are consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

# Scope

The provisions of these policies pertain to all {Insert Company Name} employees, contractors, third parties, and others who have access to company and customer confidential information within {Insert Company Name} systems and facilities.

# Roles and Responsibilities

These policies apply to all {Insert Company Name} employees, contractors, business partners, third parties, and others who need or have access to {Insert Company Name}’s systems and our customer's confidential information. {Insert Company Personnel below and delete this for final product}

|  |  |  |
| --- | --- | --- |
| **Individual or Group** | **Role** | **Responsibility** |
|  | CEO | Highest-level official with overall responsibility to develop, implement, and maintain accountability, active support, oversight, and management commitment for information security objectives. |
|  | President | Responsible for developing, implementing, maintaining, and ensuring compliance with information security policies, procedures, and controls. Has final responsibility for information security program. |
|  | Information Owner | Has statutory, management, or operational authority for {Insert Company Name} information. Responsible for developing, implementing, and maintaining policies and procedures governing information generation, collection, processing, dissemination, and disposal. |
|  | Authorizing Official | Responsible for operating information system at an acceptable level of risk to organizational operations and assets. |
| **Individual or Group** | **Role** | **Responsibility** |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | Chief Information Security Officer | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | Information Security Manager | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | Information Technology Director | Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. |
|  | Information System Security Officer | Responsible for ensuring that the appropriate operational security posture is maintained for an information system, responsible for ensuring coordination among groups is managed and maintained for these policies/procedures. |
| System Admin Team | System Administrator | Responsible for conducting information system security Administration activities. |
| Varies | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures. |
| Varies | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

{Insert Company Name} and its management are fully committed to protecting the confidentiality and integrity of corporate proprietary and production systems, facilities, and data as well as the availability of services in the {Insert Company Name} Information System by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the {Insert Company Name} Information Owner. The following applicable laws, directives, policies, regulations, and standards were used as part of the development for this policy. These include, but are not limited to:

1. E-Government Act of 2002
2. Federal Information Security Modernization Act of 2014 (FISMA)
3. The Privacy Act of 1974
4. Clinger-Cohen Act of 1996
5. OMB Circulars and Memoranda
6. Federal Information Processing Standards (FIPS)
7. NIST Special Publications
8. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
9. OMB Memorandum for Agency CIOs: Security Authorization of Information Systems in Cloud Computing Environments, December 2011

# Compliance

Compliance with these policies is mandatory. It is {Insert Company Name}’s policy that production systems meet or exceed the requirements outlined in this document. The Information Owner will periodically assess compliance with these policies by using an independent audit performed by an external vendor and/or internal self-assessments to identify areas of non-compliance. Any findings identified in the audit will be remediated in accordance with the auditing team’s recommendations.

# Policy Requirements

The following personally identifiable information processing and transparency controls requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support information systems owned and operated by {Insert Company Name}, including its subsidiaries and affiliates, collectively referred to as {Insert Company/Product Name}.

The following access control requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the {Insert Company/Product Name} information systems.

8.1 System and Communications Protection Policies and Procedures [SC-1]

This document is intended to serve as the System and Communication Protection Policy and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the System and Communication Protection Policy and related controls have been developed, documented, and disseminated to all applicable personnel.

{Insert Company Name} must develop, document, and disseminate to all personnel including the chief privacy officer, ISSO, and/or similar roles or their designees: [SC-1 (a)]

* An organizational-level System and Communication Protection Policy that: [SC-1 (a) (1)]
  + Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance [SC-1 (a) (1) (a)]
  + Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines [SC-1 (a) (1) (b)]
* Procedures to facilitate the implementation of System and Communication Protection Policy and the associated System and Communication Protection controls [SC-1 (a) (2)]

{Insert Company Name} must designate a Chief Information Security Officer (CISO) to manage the development, documentation, and dissemination of the System and Communication Protection policy and procedures. [SC-1 (b)]

{Insert Company Name} must review and update the current System and Communication Protection: [SC-1 (c)]

* Policies at least annually, following a significant change, and/or any compromising event [SC-1 (c) (1)]
* Procedures at least annually, following a significant change, and/or any compromising event [SC-1 (c) (2)]

8.2 Separation of System and User Functionality [SC-2]

{Insert Company Name} must separate user functionality, including user interface services, from system management functionality.

8.3 Security Function Isolation [{Sc-3 High Only}]

**For high impact systems only:**

{Insert Company Name} must ensure that security functions are isolated from non-security functions by applying the systems security engineering design principles from SA-8.

8.4 Information in Shared System Resources [SC-4]

{Insert Company Name} must ensure the Information System prevents unauthorized and unintended information transfer via shared system resources.

8.5 Denial of Service Protection [SC-5]

{Insert Company Name} must ensure the information system protects against the effects of denial of service (DoS) attacks, including, at a minimum: ICMP (ping) floods, SYN floods, slowloris, buffer overflow attacks, and volume attacks.

8.6 Boundary Protection [SC-7, SC-7 (3,4,5,7,8,12,18), {SC-7 (10,20,21) High Only}]

To protect the information system boundaries, {Insert Company Name} must:

* Monitor and control communications at the external managed interfaces of the system and at key internal managed interfaces within the system [SC-7 (a)]
* Implement subnetworks for publicly accessible information system components that are physically and/or logically separated from internal organizational networks [SC-7 (b)]
* Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the {Insert Company Name} security and privacy architecture [SC-7 (c)]

Access Points:

* Limit the number of external network connections to the information system [SC-7 (3)]

External Telecommunications Services:

* Implement a managed interface for each external telecommunication service [SC-7 (4) (a)]
* Establish a traffic flow policy for each managed interface [SC-7 (4) (b)]
* Employ security controls as needed to protect the confidentiality and integrity of the information being transmitted across each managed interface [SC-7 (4) (c)]
* Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need [SC-7 (4) (d)]
* Review exceptions to the traffic flow policy at least every ninety (90) days for high impact systems or 180 days for all others or whenever there is a change in the threat environment that warrants a review of the exceptions and remove traffic flow policy exceptions that are no longer supported by an explicit mission or business need [SC-7 (4) (e)]
* Prevent unauthorized exchange of control plane traffic with external networks [SC-7 (4) (f)]
* Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks [SC-7 (4) (g)]
* At managed interfaces, deny network traffic by default and allow network communications traffic by exception on any system (e.g. deny all or permit by exception) [SC-7 (5)]
* Prevent split tunneling for remote devices connection to organizational systems unless the split tunnel is securely provisioned using established VPN [SC-7 (7)]
* Route traffic from the Information System to any network outside of organizational control and any network outside the authorization boundary through authenticated proxy servers within the managed interfaces of boundary protection devices [SC-7 (8)]
* Implement a Host Intrusion Prevention Systems (HIPS), Host Intrusion Detection System (HIDS), or at minimum a host-based firewall on all virtual machines within the system components [SC-7 (12)]
* Prevent systems from entering unsecure state in the event of an operational failure of a boundary protection device [SC-7 (18)]

**For high impact systems only:**

* Prevent the exfiltration of information and conduct exfiltration tests at least annually [SC-7 (10)]
* Provide the capability to dynamically isolate any system components from other system components [SC-7 (20)]
* Employ boundary protection mechanisms to isolate infrastructure supporting each {Insert Company Name} product and business functions [SC-7 (21)]

8.7 Transmission Confidentiality and Integrity [SC-8, SC-8 (1)]

{Insert Company Name} must ensure that the information system protects the confidentiality and integrity of transmitted information by employing cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by alternative physical measures. [SC-8, SC-8 (1)]

{Insert Company Name} requires the use of cryptography which must be compliant with government requirements and utilize FIPS validated or NSA approved cryptography (see NIST SP 800-53 SC-8 (5), SC-8 (1), SC-13) for systems processing Federal government data. [SC-8 (1)]

{Insert Company Name} must verify encryption is properly configured in all IaaS/PaaS implementations. {Insert Company Name} must document cryptographic module implementation, including Data at Rest (DAR) and Data in Transit (DIT), in the application System Security Plan, if applicable. [SC-8 (1)]

8.8 Network Disconnect [SC-10]

{Insert Company Name} must ensure that the information system terminates the network connection associated with a communications session at the end of the session or after ten (10) minutes of inactivity for privileged sessions and no longer than fifteen (15) minutes of inactivity for user sessions. [SC-10]

8.9 Cryptographic Key Establishment & Management [SC-12, {SC-12 (1) High Only}]

{Insert Company Name} must establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management guidance: FIPS 140-3, SP 800-56A, SP 800-56B, SP 800-56C, SP 800-57-1, SP 800-57-2, SP 800-57-3, SP 800-63-3, IR 7956, and IR 7966. {Insert Company Name} must produce, control, and distribute symmetric cryptographic keys using NIST-approved key management technology. {Insert Company Name} must produce, control, and distribute asymmetric cryptographic keys using approved PKI Class 3 (or better) certificates. [SC-12]

**For high impact systems only:**

{Insert Company Name} must maintain availability of information in the event of the loss of cryptographic keys by users. [SC-12 (1)]

8.10 Cryptographic Protection [SC-13]

{Insert Company Name} must determine the use cases of cryptography; examples include encryption and decryption of data, generation of one-time passwords (OTPs) for MFA, and protocols such as TLS, SSH, and HTTPS.

For Federal data, {Insert Company Name} must use FIPS-validated or NSA-approved cryptography that complies with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The requirement for FIPS 140 validation, as well as timelines for acceptance of FIPS 140-2, and 140-3 can be found at the NIST Cryptographic Module Validation Program (CMVP). [SC-13]

8.11 Collaborative Computing Devices and Applications [SC-15]

For systems hosting {Insert Company Name} products, {Insert Company Name} must prohibit remote activation of collaborative computing devices and applications with no exceptions. In all cases the device must provide an explicit indication of use to users physically present at the device. [SC-15]

8.12 Public Key Infrastructure Certificates [SC-17]

{Insert Company Name} must issue public key certificates under an organization-controlled certificate authority within the information system boundary or obtain public key certificates from an approved third-party service provider. [SC-17 (a)]

{Insert Company Name} must include only approved trust anchors in trust stores or certificate stores managed by the organization. [SC-17 (b)]

8.13 Mobile Code [SC-18]

{Insert Company Name} must define acceptable and unacceptable mobile code technologies (e.g. JavaScript, ActiveX, VBScript, etc.) and authorize, monitor, and control the use of mobile code within the system. [SC-18]

8.14 Secure Name/Address Resolution Service (Authoritative Source) [SC-20]

{Insert Company Name} must ensure that the information system utilizes DNS Security Extensions (DNSSEC) to provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries. Authoritative DNS servers must be geolocated within the U.S./U.S. Territories or geographic locations where there is U.S. jurisdiction. External authoritative DNS servers may be located outside an authorized environment. How ever positioning these servers inside an authorized boundary is encouraged. {Insert Company Name} must verify the DNSSEC configuration through one of many available analyzers. When operating as part of a distributed, hierarchical namespace, {Insert Company Name} must provide the means to indicate the security status of child zones and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains. [SC-20]

8.15 Secure Name/Address Resolution Service (Recursive or Caching Resolver) [SC-21]

{Insert Company Name} must ensure that the information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.

Procedures should include how DNSSEC is implemented on recursive DNS servers to make DNSSEC requests when resolving DNS requests from internal components to domains external to the boundary.

This includes handling signed and unsigned replies. Note: Accepting an unsigned reply is acceptable.

Internal recursive DNS servers must be located inside an authorized environment or leveraged from an underlying IaaS/PaaS. DNSSEC resolution to access a component inside the boundary is excluded. [SC-21]

8.16 Architecture and Provisioning for Name/Address Resolution Service [SC-22]

{Insert Company Name} must ensure that the Domain Name System (DNS) providers that collectively provide name/address resolution service for the information system are fault-tolerant and implement internal/external role separation. [SC-22]

8.17 Session Authenticity [SC-23]

{Insert Company Name} must ensure that the information system provides mechanisms to protect the authenticity of communications sessions. Authenticity protection includes protecting against man-in-the-middle attacks, session hijacking, and the insertion of false information into sessions. [SC-23]

8.18 Fail in Known State [{SC-24 High Only}]

**For high impact system only:**

{Insert Company Name} must ensure to fail (roll back) to last known safe state while preserving system state information for the following failures on the indicated components (including, but not limited to): [SC-24]

* Data corruption
* Data poisoning
* Failed patch/upgrade/change
* Failed system reallocation
* Malware/Ransomware
  1. Protection of Information at Rest [SC-28, SC-28 (1)]

{Insert Company Name} must ensure that information systems protect the confidentiality and integrity of data at rest, including but not limited to: [SC-28]

* Back-ups
* Cloud storage of non-public data
* Removable media
* Mobile device media
* Sensitive database fields
* All information system components storing data that must be protected at the High or Moderate impact levels

{Insert Company Name} must support the use of cryptographic mechanisms to prevent unauthorized disclosure and modification of data on system components storing data. {Insert Company Name} has the responsibility to verify encryption is properly configured. [SC-28 (1)]

* 1. Process Isolation [SC-39]

{Insert Company Name} must maintain a separate execution domain for each executing system process. Process isolation technologies include: [SC-39]

* Sandboxing
* Virtualization
* Logically separate software and firmware from other software, firmware, and data.
  1. System Time Synchronization [SC-45, SC-45 (1)]

{Insert Company Name} must synchronize system clocks within and between systems and system components. [SC-45]

All {Insert Company Name} information systems and components shall:

* Compare the internal system clocks at least hourly with NIST internet time service [SC-45 (1) (a)]
* Synchronize the internal system clocks to the authoritative time source when the time difference is greater than zero [SC-45 (1) (b)]