

{Insert Company Name}

Security Policy

System and Information Integrity

**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[Document Revision History 0](#_Toc188619802)

[Table of Contents 1](#_Toc188619803)

[1 Introduction 0](#_Toc188619804)

[2 Purpose 0](#_Toc188619805)

[3 Scope 0](#_Toc188619806)

[4 Roles and Responsibilities 0](#_Toc188619807)

[5 Management Commitment 1](#_Toc188619808)

[6 Authority 2](#_Toc188619809)

[7 Compliance 2](#_Toc188619810)

[8 Policy Requirements 0](#_Toc188619811)

[8.1 System and Information Policies and Procedures [SI-1] 0](#_Toc188619812)

[8.2 Flaw Remediation [SI-2, SI-2 (2,3)] 0](#_Toc188619813)

[8.3 Malicious Code Protection [SI-3] 1](#_Toc188619814)

[8.4 System Monitoring [SI-4, SI-4 (1,2,4,5,16,18,23), {SI-4 (10,11,12,14,19,20,22) High Only}] 1](#_Toc188619815)

[8.5 Security Alerts, Advisories, and Directives [SI-5] 2](#_Toc188619816)

[8.6 Security and Privacy Function Verification [SI-6] 3](#_Toc188619817)

[8.7 Software, Firmware, & Information Integrity [SI-7, SI-7 (1,7), {SI-7 (2,5,15) High Only}] 3](#_Toc188619818)

[8.8 Spam Protection [SI-8, SI-8 (2)] 3](#_Toc188619819)

[8.9 Information Input Validation [SI-10] 4](#_Toc188619820)

[8.10 error Handling [SI-11] 4](#_Toc188619821)

[8.11 Information Management and Retention [SI-12] 4](#_Toc188619822)

[8.12 Memory Protection [SI-16] 4](#_Toc188619823)

# 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 Information Policies and Procedures [SI-1]

This document is intended to serve as the *System and Information Integrity Policy* and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *System and Information Integrity 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: [SI-1 (a)]

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

{Insert Company Name} must review and update the current System and Information Integrity: [SI-1 (c)]

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

8.2 Flaw Remediation [SI-2, SI-2 (2,3)]

{Insert Company Name} must:

* Identify, report, and correct information system flaws [SI-2 (a)]
* Test software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation [SI-2 (b)]
* Install security relevant software and firmware updates within 30 days of release updates [SI-2 (c)]
* Incorporate flaw remediation into the organizational configuration management process [SI-2 (d)]
* Determine if system components have applicable security-relevant software and firmware updates installed using automated scanning mechanisms at least monthly to determine the status of known flaws for system components [SI-2 (2)]
* Measure the time between flaw identification and remediation [SI-2 (3) (a)]
* Establish a benchmark, on the average time it takes from flaw identification to corrective actions and remediation [SI-2 (3) (b)]

8.3 Malicious Code Protection [SI-3]

{Insert Company Name} must:

* Implement signature based and non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code [SI-3 (a)]
* Ensure that the system automatically updates malicious code protection mechanisms as new releases are available in accordance with configuration management policy and procedures [SI-3 (b)]
* Configure malicious code protection mechanisms to: [SI-3 (c)]
* Perform periodic scans of the system at least weekly and real-time scans of files from external sources at multiple points including endpoints, network entry, and network exit points as the files are downloaded, opened, or executed in accordance with organizational policy [SI-3 (c) (1)]
* Block and quarantine malicious code and alert administrator or security personnel in near-real time in response to malicious code detection [SI-3 (c) (2)]
* Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system [SI-3 (d)]

8.4 System Monitoring [SI-4, SI-4 (1,2,4,5,16,18,23), {SI-4 (10,11,12,14,19,20,22) High Only}]

{Insert Company Name} must:

* Monitor the information system to detect: [SI-4 (a)]
  + Attacks and indicators of potential attacks consistent with US-CERT Incident Response Reporting Guidelines [SI-4 (a) (1)]
  + Unauthorized local, network, and remote connections [SI-4 (a) (2)]
* Identifies unauthorized use of the system through monitoring system boundaries and alerting based on activity in the information audit logs [SI-4 (b)]
* Invoke internal monitoring capabilities or deploy monitoring devices: [SI-4 (c)]
  + Strategically within the system to collect organization-determined essential information [SI-4 (c) (1)]
  + At ad hoc locations within the system to track specific types of transactions of interest to the organization [SI-4 (c) (2)]
* Analyze detected events and anomalies [SI-4 (d)]
* Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information to include privileged users [SI-4 (e)]
* Obtain legal opinion regarding system monitoring activities in accordance with applicable state and federal laws, Executive Orders, directives, policies, or regulations [SI-4 (f)]
* Provide audit system monitoring logs to the {Insert Company Name} Technology Team as needed on a continual basis [SI-4 (g)]
* Connect and configure individual intrusion detection tools into a system-wide intrusion detection system [SI-4 (1)]
* Employ automated tools to support near real-time analysis of events [SI-4 (2)]
* Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communication traffic [SI-4 (4) (a)]
* Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions [SI-4 (4) (b)]
* Alert IS/IT personnel when the following system-generated indications of compromise or potential compromise occur in accordance with the Incident Response Plan [SI-4 (5)]:
  + Audit records
  + Inputs from malicious code protection mechanisms
  + Intrusion detection or prevention mechanisms
  + Boundary protection devices such as firewalls, gateways, and routers
* Correlate information from monitoring tools employed throughout the system [SI-4 (16)]
* Analyze outbound communications traffic to detect covert exfiltration of information which may include steganography at external interfaces to the system and at interior points to include but not limited to: [SI-4 (18)]
  + Subnets
  + VLANs
  + Routers
  + Endpoints
  + Gateways
  + Firewalls
* Implement host-based monitoring mechanisms on servers, notebook computers, and mobile devices. {Insert Company Name} may employ host-based monitoring mechanisms from multiple product developers or vendors including antivirus, HIPS, and MDM. [SI-4 (23)]

**For high impact systems only:**

* Make provisions so that all encrypted communications traffic is visible to internal and external inspection tools to provide support to agency requirements to comply with M-21-3 [SI-4 (10)]
* Analyze outbound communications traffic at the external interfaces to the system to discover anomalies [SI-4 (11)]
* Alert using text and/or email alerts when the following indications of inappropriate or unusual activities from predetermined security or privacy implications [SI-4 (12)]
* Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system [SI-4 (14)]
* Implement additional monitoring of individuals who have been identified by management or Human Resources as posing an increased level of risk. **[SI-4 (19)]**
* Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring]. **[SI-4 (20)]**
* Detect network services that have not been authorized or approved by Change Management Board or designated personnel; and **[SI-4 (22) (a)]**
* Alert Information Security when detected. **[SI-4 (22) (b)]**

8.5 Security Alerts, Advisories, and Directives [SI-5]

{Insert Company Name} must:

* Receive information system security alerts, advisories, and directives from US-CERT and on an ongoing basis
* Generate internal security alerts, advisories, and directives as deemed necessary
* Disseminate security alerts, advisories, and directives to system security personnel and administrators with patch-management responsibilities
* Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance
* Broadcast security alert and advisory information throughout the organization using

8.6 Security and Privacy Function Verification [SI-6]

{Insert Company Name} must ensure that the information system will:

* Verify the correct operation of security and privacy functions [SI-6 (a)]
* Perform this verification of the functions specified in SI-6a during system startup and/or restart, and upon command by user with appropriate privilege at least monthly [SI-6 (b)]
* Notify the Information Security team and system administrators of failed security verification tests [SI-6 (c)]
* Shut down or restart the information system or affected component and notify the Information Security team and the IT team when anomalies are discovered [SI-6 (d)]

8.7 Software, Firmware, & Information Integrity [SI-7, SI-7 (1,7), {SI-7 (2,5,15) High Only}]

{Insert Company Name} must:

* Check the information system integrity by employing verification tools to detect unauthorized changes due to errors or malicious activity to the system baseline software, firmware, and information [SI-7 (a)]
* When unauthorized changes to the software, firmware, and information are detected, take-action by (one or more of the following): [SI-7 (b)]
  + Generating an alert to the Information Security Team or appropriate personnel
  + Automated remediation
  + Initiate the Incident Response Plan
* Perform an integrity check of the device’s software, firmware, and information, at startup, at security-relevant event, or at least monthly [SI-7 (1)]
* Incorporate the detection of unauthorized changes in the software, firmware, and information into the Incident Response capability [SI-7 (7)]

**For high impact systems only:**

* Employ automated tools that provide notification to the ISSO and/or {Insert Company Name} Technology Team upon discovering discrepancies during integrity verification [SI-7 (2)]
* Automatically shut down or restart the system, lock the offending account, or initiate other appropriate actions when integrity violations are discovered [SI-7 (5)]
* Implement cryptographic mechanisms to authenticate all software and firmware components inside the boundary prior to installation [SI-7 (15)]

8.8 Spam Protection [SI-8, SI-8 (2)]

{Insert Company Name} must:

* Employ centrally managed spam protection mechanisms at information system entry and exit points to detect and act on unsolicited messages [SI-8 (a)]
* Update spam protection mechanisms automatically (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures [SI-8 (b)]
* Automatically update spam protection mechanisms continuously. [SI-8 (2)]

8.9 Information Input Validation [SI-10]

{Insert Company Name} must ensure that information systems check the validity of information inputs and that all inputs are valid and document any exceptions.

8.10 error Handling [SI-11]

{Insert Company Name} must ensure that information systems:

* Generates generic error messages that provide information necessary for corrective actions without revealing information that could be exploited [SI-11 (a)]
* Reveal verbose error messages only to {Insert Company Name} Technology Team members involved in remediating errors. Note this may include notification to the agency ISSO [SI-11 (b)]

8.11 Information Management and Retention [SI-12]

{Insert Company Name} must manage and retain information within the system and information output from the system in accordance with applicable federal laws, state laws, executive orders, directives, policies, regulations, standards, guidelines, and operational requirements.

8.12 Memory Protection [SI-16]

{Insert Company Name} must implement OS data execution protections to protect the system memory from unauthorized code execution.