

{Insert CompanY Name}

Security Procedures

System and Information Integrity (SI)

**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 1](#_Toc152925467)

[Table of Contents 2](#_Toc152925468)

[1 Introduction 3](#_Toc152925469)

[2 Purpose 3](#_Toc152925470)

[3 Scope 3](#_Toc152925471)

[4 Roles and Responsibilities 3](#_Toc152925472)

[5 Management Commitment 4](#_Toc152925473)

[6 Authority 5](#_Toc152925474)

[7 Compliance 5](#_Toc152925475)

[8 Procedural Requirements [SI-1] 6](#_Toc152925476)

[8.1 Flaw Remediation [SI-2] 6](#_Toc152925477)

[8.2 Malicious Code Protection [SI-3] 6](#_Toc152925478)

[8.3 Information System Monitoring [SI-4] 6](#_Toc152925479)

[8.4 Security Alerts, Advisories, and Directives [SI-5] 6](#_Toc152925480)

[8.5 Security Functionality Verification [SI-6] 7](#_Toc152925481)

[8.6 Software & Information Integrity [SI-7] 7](#_Toc152925482)

[8.7 Spam Protection [SI-8] 7](#_Toc152925483)

[8.8 Input Validation, Error Handling, Output, and Retention [SI-10, SI-11, SI-12] 7](#_Toc152925483)

[8.9 Memory Protection {SI-16] 7](#_Toc152925483)

# Introduction

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

# Purpose

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

# Scope

The provisions of these procedures 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 procedures 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** |
| {Insert Individual Name} | CEO | Highest-level official with overall responsibility to develop, implement, and maintain accountability, active support, oversight, and management commitment for information security objectives. |
| {Insert Individual Name} | President | Responsible for developing, implementing, maintaining, and ensuring compliance with information security policies, procedures, and controls. Has final responsibility for information security program. |
| {Insert Individual Name} | 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. |
| **Individual or Group** | **Role** | **Responsibility** |
| {Insert Individual Name} | Authorizing Official | Responsible for operating information system at an acceptable level of risk to organizational operations and assets. |
| {Insert Individual Name} | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
| {Insert Individual Name} | 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. |
| {Insert Individual Name} | Information Security Manager | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
| {Insert Individual Name} | Information Technology Director | Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. |
| {Insert Individual Name} | 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. |
| {Insert Individual or Team Name} | 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 procedures is mandatory. It is {Insert Company Name} policy that production systems meet or exceed the requirements outlined in this document. The Information Owner will periodically assess compliance with these procedures 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.

# Procedural Requirements [SI-1]

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

8.1 Flaw Remediation [SI-2]

The {Insert Individual or Team Name} is responsible for implementing vulnerability scanning for the purpose of identifying, reporting on, and remediating information system flaws.

{Insert Company Name} utilizes {Insert names of implemented vulnerability scanning tools} to perform {Provide details on scan types performed and the systems or applications the scans are performed on}.

{State how vulnerabilities discovered are monitored, this could include console dashboards, reporting, or console queries}

{State how vulnerabilities discovered in company developed products are tracked, prioritized, and remediated. This could include console dashboards or project management tools used for tracking flaws}

{State how infrastructure vulnerabilities discovered are tracked, prioritized, and remediated. This could include console dashboards or project management tools used for tracking flaws. Products used to remediate vulnerabilities could include Configuration Management tools, policy management tools, or other application management tools} [SI-2 (a)]

{State how software and application updates are tested prior to being installed or deployed to the production environment} [SI-2 (b)]

{State vulnerability remediation timelines for High, Medium, and Low vulnerabilities}

{State how vulnerability remediation is automatically verified. Provide timelines of the frequency of vulnerability scanning to verify vulnerability remediation.} [SI-2 (2)] {State how the time between flaw identification and remediation is measure for the Information System} [SI-2 (3) (a)]

{State how the organization establishes the benchmark on the average time it takes from flaw identification to flaw remediation} [SI-2 (3) (b)]

{State how flaw remediation is incorporated with the organization’s configuration management tool. Include details on how flaw remediation change requests are opened, approved, reviewed, and closed} [SI-2 (d)]

{Insert inherited control language if applicable}

8.2 Malicious Code Protection [SI-3]

{Insert Company Name} has deployed {State the product names that provide signature based and non-signature based malicious code protection and where these tools are deployed to protect the Information System} [SI-3 (a)] {State features enabled within the deployed malicious code protection tools and how these features protect the environment}

{State how malicious code protection signatures are updated. Provide the update frequency on clients within the environment and the update frequency of the signature update source if applicable. State the update source for clients in the environment and the update source for the signature source.} [SI-3 (b)] {State how malicious code protection applications are updated.}

{Provide scan frequencies for malicious protection applications. State if real-time scanning is enabled in the environment and how real-time scanning is configured.} [SI-3 (c) (1)] If malicious code is identified, {State actions taken to block or contain the malicious code} and an alert is sent {Insert how the alert is sent (examples include but are not limited to: through an e-mail message, through a SMS message, and displayed within a monitored console)} to {Insert Individual or Team Name}. [SI-3 (c) (2)] {State actions taken to review malware events for potential false positives. What does the organization do with the false positive? Is the file restored, sent to the vendor, or is some other action taken with the false positive file(s)?} [SI-3 (d)]

{State how malicious code protection tools are initially released to system within the environment and updated} {State how events from malicious code protection tools and clients within the environment are collected}

{Insert inherited control language if applicable}

8.3 Information System Monitoring [SI-4]

{Insert Company Name} shall require the following:

* 1. Monitor the system to detect: [SI-4 (a)]
     1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: {organization-defined monitoring objectives}
     2. Unauthorized local, network, and remote connections
  2. Identify unauthorized use of the system through the following techniques and methods: {organization-defined techniques and methods} [SI-4 (b)]
  3. Invoke internal monitoring capabilities or deploy monitoring devices: [SI-4 (c)]
     1. Strategically within the system to collect organization-determined essential information
     2. At ad hoc locations within the system to track specific types of transactions of interest to the organization
  4. Analyze detected events and anomalies [SI-4 (d)]
  5. 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 [SI-4 (e)]
  6. Obtain legal opinion regarding system monitoring activities [SI-4 (f)]
  7. Provide {Insert organization-defined SIEM} to {Insert Individual or role} {Selection (as needed or organization-defined frequency)}. [SI-4 (g)]

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

{Insert Company Name} shall require the following:

1. Receive system security alerts, advisories, and directives from {to include US-CERT and Cybersecurity and Infrastructure Security Agency (CISA) Directives} on an ongoing basis [SI-5 (a)]
2. Generate internal security alerts, advisories, and directives as deemed necessary [SI-5 (b)]
3. Disseminate security alerts, advisories, and directives to: {Select: (to include system security personnel and administrators with configuration/patch-management responsibilities) or (organization-defined elements within the organization) or (organization-defined external organizations)} [SI-5 (c)]
4. Implement security directives in accordance with established time frames or notify the issuing organization of the degree of noncompliance [SI-5 (d)]

8.5 Security Functionality Verification [SI-6]

{Insert Company Name} shall require the following:

1. Verify the correct operation of {organization-defined security and privacy control language} [SI-6 (a)]
2. Perform the verification of the functions specified in SI-6a {Select (one-or-more) (system transitional states to include upon system startup and/or restart)} or {(upon command by user with appropriate privilege)} and at least monthly [SI-6 (b)]
3. Alert {Insert Individual or Team Name} to include system administrators and security personnel to failed security and privacy verification tests [SI-6 (c)]
4. {Select (one-or-more) (Shut the system down) or (Restart the system) or (alternative actions(s) organization-defined)} when anomalies are discovered. [SI-6 (d)]

8.6 Software & Information Integrity [SI-7]

{Insert Company Name} shall require the following:

1. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information {organization-defined control language (e.g., software, firmware, and information)} [SI-7 (a)]
2. Take the following actions when unauthorized changes to the software, firmware, and information are detected {organization-defined actions}. [SI-7 (b)]

8.7 Spam Protection [SI-8]

{Insert Company Name} shall require the following:

1. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages [SI-8 (a)]
2. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures [SI-8 (b)]

8.8 Input Validation, Error Handling, Output, and Retention [SI-10, SI-11, SI-12]

{Insert Company Name} must:

Check the validity of the following information inputs {organization-defined information inputs to the system}. [SI-10]

{Insert Company Name} must:

1. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited [SI-11 (a)]
2. Reveal error messages only to {Organization-defined roles (e.g., the ISSO and/or similar role within the organization)}. [SI-11 (b)]

{Insert Company Name} must:

Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. [SI-12]

8.9 Memory Protection [SI-16]

{Insert Company Name} shall require the following:

Implement the following controls to protect the system memory from unauthorized code execution {organization-defined control(s)}.