Insert Logo Here

Organization Name

Security Policy

System & Information Integrity

Version 1.0

April 6, 2021

Proprietary and Confidential

For Authorized Use Only

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 4/6/2021 | 1.0 | Published SI Policy | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68594754)

[2 Purpose 1](#_Toc68594755)

[3 Scope 1](#_Toc68594756)

[4 Roles and Responsibilities 1](#_Toc68594757)

[5 Management Commitment 2](#_Toc68594758)

[6 Authority 3](#_Toc68594759)

[7 Compliance 3](#_Toc68594760)

[8 Policy Requirements 4](#_Toc68594761)

[8.1 System and Information Integrity Policies and Procedures 4](#_Toc68594762)

[8.2 Flaw Remediation 4](#_Toc68594763)

[8.3 Malicious Code Protection 4](#_Toc68594764)

[8.4 Information System Monitoring 5](#_Toc68594765)

[8.5 Security Alerts & Advisories 6](#_Toc68594766)

[8.6 Security Functionality Verification 6](#_Toc68594767)

[8.7 Software, Firmware, & Information Integrity 6](#_Toc68594768)

[8.8 Spam Protection 6](#_Toc68594769)

[8.9 Information Input Validation 7](#_Toc68594770)

[8.10 Error Handling 7](#_Toc68594771)

[8.11 Information Handling and Retention 7](#_Toc68594772)

[8.12 Memory Protection 7](#_Toc68594773)

# Introduction

Organization Name has developed corporate policies that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by Organization Name 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 4.

# Purpose

The purpose of these policies is to establish access control requirements to ensure the confidentiality, integrity, and availability of Organization Name 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 Organization Name employees, contractors, third parties, and others who have access to company and customer confidential information within Organization Name systems and facilities.

# Roles and Responsibilities

These policies apply to all Organization Name employees, contractors, business partners, third parties, and others who need or have access to Organization Name systems and our customer's confidential information.

| **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 Organization 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. |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | 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 Manager | 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 Administrator | Responsible for conducting information system security Administration activities. |
|  | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures |
|  | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

Organization 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 Organization Name system by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the Organization 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/Federal Information Security Management Act of 2002 (FISMA)
2. The Privacy Act of 1974
3. Clinger-Cohen Act of 1996
4. OMB Circulars and Memoranda
5. Federal Information Processing Standards (FIPS)
6. NIST Special Publications
7. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
8. 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 Organization Name 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 annually by an external vendor 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 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 Organization Name information systems.

## System and Information Integrity Policies and Procedures

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 physical and environmental protection controls have been developed, documented, and disseminated to all applicable personnel.

The Information Owner will review and update the *System and Information Integrity Policy* every three (3) years and the procedure(s) at least annually or any time there are significant changes in software or security. Updates must be made to keep the policy and procedure(s) in alignment with Organization Name overall business goals and risk position. Any updates, improvements, or suggestions regarding the *System and Information Integrity Policy* and/or procedure(s) must be sent to the Information Owner.

## Flaw Remediation

Organization Name must:

* Identify, report, and correct information system flaws
* Test software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation
* Install security relevant software and firmware updates within 30 days of release updates
* Incorporate flaw remediation into the organizational configuration management process
* Employ automated mechanisms at least monthly to determine the state of information components with regard to flaw remediation
* Measure the time between flaw remediation and identification
* Establish benchmarks for taking corrective action

## Malicious Code Protection

Organization Name must:

* Employ malicious code protection mechanisms at information entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code
* Ensure that information automatically updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures
* Configure malicious code protection mechanisms to:
	+ Perform periodic scans of information at least weekly in response to malicious code detection and real-time scans of files from external sources at to include endpoints as the files are downloaded, opened, or executed in accordance with organizational security policy
	+ Alert administrator or security personnel in response to malicious code detection
* Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system
* Centrally manage malicious code protection mechanisms
* Ensure information automatically updates malicious code protection mechanisms (including signature definitions)
* Implement non-signature based malicious code detection mechanisms

## Information System Monitoring

Organization Name must:

* Monitor the information system to detect attacks and indicators of potential attacks in accordance with detecting malicious activity including unauthorized access and malware and unauthorized local, network, and remote connections
* Identifies unauthorized use of information through monitoring system boundaries and alerting based on activity in the information audit logs
* Deploy monitoring devices strategically within information to collect organization-determined essential information and at ad hoc locations within the system to track specific types of transactions of interest to the organization
* Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion
* Heighten the level of information monitoring activity whenever there is an indication of increased 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
* Obtain legal opinion with regard to information monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations
* Provide audit or system monitoring logs to the ISM and On-Call Team
* Connect and configure individual intrusion detection tools into an information system-wide intrusion detection system
* Employ automated tools to support near real-time analysis of events
* Ensure that information continually monitors inbound and outbound communications traffic for unusual or unauthorized activities or conditions
* Ensure that information alerts the appropriate teams following indications of compromise or potential compromise occur, including Denial of Service, SQL Injection, Unauthorized Access Attempts, Loss of Service Availability, and Audit Logging Failures
* Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system
* Ensure that information correlates information from monitoring tools employed throughout the information system
* Implement host-based monitoring of information system components

## Security Alerts & Advisories

Organization Name must:

* Receive information system security alerts, advisories, and directives from US-CERT and other source on an ongoing basis
* Generate internal security alerts, advisories, and directives as deemed necessary
* Disseminate security alerts, advisories, and directives to system administrators, database administrators, network administrators, etc.
* Implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance

## Security Functionality Verification

Organization Name must ensure that information will:

* Verify the correction operation of organization-defined security functions
* Perform this verification upon system startup and/or restart at least monthly
* Notify system administrators and security personnel of failed security verification tests
* Shut down or restart the information system and notify system administrators and security personnel when anomalies are discovered

## Software, Firmware, & Information Integrity

Organization Name must:

* Employ integrity verification tools within the information environment to detect unauthorized changes to software and information
* Ensure that integrity checks of information software and information are performed at startup, installation, or change when systems and accounts are modified and at least monthly
* Incorporate the detection of unauthorized changes into the information incident response capability

## Spam Protection

Organization Name must:

* Employ centrally managed spam protection mechanisms at information entry and exit points to detect and act on unsolicited messages
* Update spam protection mechanisms automatically (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures
* Centrally manage spam protection mechanisms

## Information Input Validation

Organization Name must ensure that the information system checks the validity of input information inputs, and that inputs are validated for correct syntax and semantics to ensure they match specified definitions for format and content.

## Error Handling

Organization Name must ensure that information:

* Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries
* Reveals error messages only to authorized administrator personnel

## Information Handling and Retention

Organization Name must handle and retain both information within and output from information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

## Memory Protection

Organization Name must ensure that the information system implements OS data execution protections to protect its memory from unauthorized code execution.