Insert Logo Here

Organization Name

Security Procedures

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 Procedure | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68612606)

[2 Purpose 1](#_Toc68612607)

[3 Scope 1](#_Toc68612608)

[4 Roles and Responsibilities 1](#_Toc68612609)

[5 Management Commitment 2](#_Toc68612610)

[6 Authority 3](#_Toc68612611)

[7 Compliance 3](#_Toc68612612)

[8 Procedural Requirements 4](#_Toc68612613)

[8.1 Flaw Remediation 4](#_Toc68612614)

[8.2 Malicious Code Protection 4](#_Toc68612615)

[8.3 Information System Monitoring 5](#_Toc68612616)

[8.4 Security Alerts, Advisories and Directives 6](#_Toc68612617)

[8.5 Security Functionality Verification 7](#_Toc68612618)

[8.6 Software Information Integrity 7](#_Toc68612619)

[8.7 Input Validation, Error Handling, Output and Retention 7](#_Toc68612620)

[8.8 Memory Protection 8](#_Toc68612621)

# Introduction

Organization Name has developed procedures that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These procedures 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

This document defines the information system and information integrity procedures. These procedures are in place to facilitate the implementation of the System and Information Integrity Policy and associated access controls. In accordance with the policy, these procedures detail how information shall implement and maintain secure access controls on all applicable information systems.

# Scope

The provisions of these procedures 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 procedures 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.

# Procedural 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.

## Flaw Remediation

The Organization Name {Role/Team}, in coordination with the {Role/Team}, are responsible for implementing vulnerability scanning for the purpose of identifying information system flaws.

{Tools} are used for vulnerability scanning. The {Tool} is used to send inventory data to {Tool} where the inventory is analyzed for operating system, software, and configuration vulnerabilities. The {Tool} is performed through a {Tool} to perform dynamic vulnerability analysis of the information system.

Vulnerability information is available to Organization Name through {Tool} vulnerability and WAS queries, reports, or dashboards. Static web application code analysis is performed through {Tool}. Results are brought into {Tools} as {bugs/Flaws/vulnerabilities}.

The {Role/Team} tests software updates related to flaw remediation for effectiveness and to ensure there are no potential side effects to the information system prior to installation. The {Role/Team} releases software updates to the test enivronment and management systems prior to release of updates to systems associated with the production web application.

Regarding Operation System and Software vulnerabilities, {Tools} vulnerability severity levels dictate the timelines of when vulnerabilities are remediated. {Severity Level} are considered high and will be remediated within 30 days of finding the vulnerability. {Severity Level} are considered medium and will be remediated within 90 days of finding the vulnerability. {Severity Level} is considered low and will be remediated within 180 days of finding the vulnerability.

The {Role/Team}is generally responsible for vulnerability remediation, unless the vulnerability lies within a security product that {Role/Team}is not allowed to manage such as {Tools} , which are managed through {Tools}.

The {Tools} on information systems within the environment sends updated inventory information every {Frequency} to {Tools}, where the inventories are analyzed for vulnerabilities. {Tool} Web Application Scans (WAS) are performed at least monthly and in alignment with SDLC sprint cycles.

The {Role/Team}and the {Role/Team} use the {Tool} Vulnerability Management dashboard to track time elapsed between operating system and software vulnerability identification and remediation. Dashboard tiles exist that help monitor vulnerabilities over time and help to prioritize vulnerability remediation. Regarding the web application, the static code scanner application identifies vulnerabilities, which are brought into {Tool} in the form of {bugs/Flaws/vulnerabilities}.

## Malicious Code Protection

Organization Name has deployed {Tool} on all information system components, including {jump/bastion/front-end/SQL/Other} servers to detect and eradicate malicious code. The primary {Tool} used for malicious code protection is {Tool}. {Tool}has an on-access scanner that continually monitors the systems in the environment for malicious code.

{Tool}is used to protect all systems within the information system. {Tool} updates malicious code protection definitions every {Frequency} (if updated definitions are available). This configuration is done by {Explain} The {Tool} will update {Tool} signatures every {Frequency} with randomization of {Frequency} (if update definitions are available). Randomization is used to prevent all systems from checking for signature updates at the same time.

Configuration of the frequency that the {Tool}looks for updates is configured within the {Tool}policies within the {Tool}. Product updates for malicious code products are pulled by the {Tool}and a notification is sent within the {Tool}dashboard that an updated product version is available. Organization Name uses the change management process to document product updates. Organization Name {Role/Team} has configured weekly on-demand scans within the {Tool} for all systems in the environment.

Organization Name has configured {Tool}to perform real-time scans of files from external sources at information system endpoints as they are downloaded, opened, or executed. In the event that malicious code is detected or identified, the malicious code protection mechanisms shall clean the malicious code. In the event the malicious code cannot be cleaned, it will be deleted from the system. {Tool} is also configured to send notifications to the {Role/Team} if threat events occur.

In the event of a false positive threat event, and assuming the file containing the false positive does not have customer information, the {Role/Team} will send the false positive file(s) to {Tool} for analysis and to prevent future false positives. This will allow {Team/Role} to prevent the file from being cleaned or deleted with future malware signature releases. {Tool} has multiple tools that provide heuristic scans to detect non-signature based malicious code.

## Information System Monitoring

TheOrganization Name {Role/Team}is responsible for identifying any unauthorized use of the information system by reviewing auditing, alerting, and reporting of the information system status. The {Role/Team}is responsible for implementing and maintaining mechanisms and processes to detect information system attacks including unauthorized local, network, remote connections and internal monitoring of assists and devices.

{Tools} send events to {Tool} thereby acting as monitoring devices, which are configured to log all malicious activity events, including unauthorized local, network, and remote connections. The {Role/Team} monitors the {Tool} for the information system environment. The {Tool} dashboards have been configured to display {Tool} Application Control and {Tool} threat events. Suspicious events generate alarms and notifications to {Role/Team} via email. Network alerts to the {Role/Team} are set up in {Tool}.

The {Role/Team} and {Role/Team} reviews implemented processes and controls (including segregation of duties) to ensure they are functioning properly and compliant with regulatory requirements. The {Role/Team} reviews weekly audit records and monthly scan reports to ensure the system is functioning in an optimal resilient and secure state. The {Role/Team} uses {Tool} , which monitors {Tools} and changes to sensitive data fields to identify unauthorized use of the information system. The {Role/Team}in coordination with {Role/Team} is responsible for identifying irregularities that are indicators of system malfunction or compromise.

The intrusion monitoring and prevention tool used for the information system is {Tool}. {Tool} will be set to prevent high severity matches on the rule signatures. {Tool} will log all medium, low, and informational matches on the {Tool} rule signatures. {Tool} events are stored in the {Tool}. Access to the {Tool} is limited to authorized members of the {Role/Team}and {Role/Team}. The {Tool} is backed up to {Hosting/Region} every {Frequency}. {Tool} events will be viewed by the {Role/Team} via {Tool}. {Tool} is displaying the logs contained within {Tool}.

Organization Name is responsible for ensuring that monitoring devices are deployed at key external and internal boundaries and within critical platform applications to collect essential information locations within the system in order to track specific types of transactions considered to be of interest. Organization Name shall provide information system monitoring data to key stakeholders as needed.

Organization Name heightens the level of monitoring for the information system by monitoring {Tool} for similarities between reported events and U.S. Cert attack types in the most recently published alerts. Organization Name consults in-house counsel for legal opinion with regard to information system monitoring activities.

Organization Name uses {Tool} to support near real-time analysis of events. {Tool} reports on malicious events as files are downloaded, copied, or opened, as well as conducting weekly full system scans. Malicious events immediately generate an alert that is sent to the {Role/Team} via email, as well as forward the event to {Tool} to allow for cross-examination of other alerts received in the environment to enable real-time analysis across the entire platform.

Organization Name uses {Tool} (malware protection and firewall), {Tool} (Application Control and Access Protection and Change Control), {Tool} (host intrusion prevention or monitoring), {Tool} (SIEM), Azure {Tool} flows (Traffic monitoring) to identify unauthorized remoted connections, potential attack attempts, and potential compromises or breaches to the system. The {Role/Team}is notified via {Tool} alerts when events (for example, when new systems are built) are discovered.

{Tool}, in coordination with {Tool} and {Tool}, are employed on all systems within the information system. These products are initially deployed to new systems via {Tool}. {Tool} and {Tool} are monitored by the {Role/Team} and provide alert capabilities when anomalies are discovered.

The information system alerts the {Role/Team} via email when all security-related indications of compromise occur. Specific alerts include:

* Unauthorized use of {Tool} Administrator accounts

## Security Alerts, Advisories and Directives

The {Role/Team} and {Role/Team} are subscribed to US-CERT RSS feeds via {Alerting/Messaging Medium} The {Role/Team} receive alerts provided by the US-CERT on an hourly RSS query. The RSS feed subscription is managed by the {Role/Team}. Organization Name {Role/Team} creates and distributes internal security alerts, advisories, or directives as deemed necessary based on US CERT alerts. These alerts would be generated in the event of a high severity vulnerability that is valid for products used within the information system.

The Organization Name {Role/Team} is responsible for ensuring that security directives are implemented within established timeframes or notifying the issuing organization of the degree of noncompliance. All information system customers are notified based on the terms and conditions of their contract with Organization Name.

## Security Functionality Verification

Security functions are verified through {Tool} via the {Tool}. The status check shows agent communication, antivirus update version, and module status including HIPS, firewall, application control, file integrity, and logging. The {Tool} dashboards are reviewed at least monthly to verify correct operation of the {Tool}. {Tool}is reviewed monthly to verify systems within the information system are communicating with {Tool}.

New systems have the {Tool}and {Tool}deployed automatically via {Tool}. {Tool}security products such as {Insert modules} are deployed via {tags/Collection} if the software is missing from a system. If the security verification tests or health checks fail, {Role/Team} or {Role/Team} is alerted, and the issue is remediated.

When anomalies are discovered in the information system, {Role/Team} or {Role/Team} personnel (depending on where the anomaly exists) will investigate the issue and determine if it is appropriate to shut down or reboot the system and conduct root cause analysis on a security functionality failure.

## Software Information Integrity

Organization Name uses {Tool}to detect unauthorized changes to the information system. The {Tool} tracks changes continuously to file and registry keys, as well as identifying who made the change. {Tool} protects critical system files, directories, and registry keys from tampering. {Tool} is used to block new software to systems in the environment.

If a legitimate change is needed to files, directories, or registry keys, then Application Control will be used to allow those changes. The change request process will be followed to enable changes to application control for these changes. All events from these {Tools} are sent to {Tool} for the {Role/Team}to review.

Organization Name performs integrity checks on all software and files using {Tool}. When Organization Name updates any information on servers, {Tool} are updated to allow changes to be made to the server. Upon completion of the updates, the {Tool} are updated to block changes, enabling the application control product.

Any attempted change to a server baseline while application control is not in an ‘Update’ mode, results in the attempted change being blocked and an email alert generated to the {Role/Team}from the {Tool}. {Tool} alerts will still run and alert the {Role/Team} on changes even while the system is in ‘update’ mode.

## Input Validation, Error Handling, Output and Retention

The Organization Name {Role/Team} performs static code scans via {Tool}. Additionally, {Role/Team} performs the static code analysis multiple times a week in the development environment, against the branch. Subsequently, the scans are scheduled every other week on release branch prior to being pushed to production. The static code scans are performed to identify any of the OWASP 10 and CWE top 25 and some of {Tools} custom security rules. For input validation, the system checks the data for file upload and character validation.

Organization Name {Role/Team} has configured information system not to expose error information. Anytime an unhandled exception occurs, the user is routed to a standard error page. Organization Name only identify potentially security-relevant error conditions, screening error messages for sensitive or confidential information and revealing messages only to authorized personnel. The error messages do not reveal:

* Username and password combinations
* Attributes used to validate a password reset request (e.g. security questions)
* Personally identifiable information (excluding unique username identifiers provided as a normal part of a transactional record)
* Biometric data or personal characteristics used to authenticate identity
* Sensitive financial records (e.g. account numbers, access codes)
* Content related to internal security functions (e.g. private encryption keys, white list or blacklist rules, object permission attributes and settings)

Additionally, Organization Name leverages {Tool} to push stack trace and error exception logs for the {Role/Team}to review and troubleshoot on the back end.

Error messages are revealed only to authorized personnel who have successfully authenticated and for whom the appropriate role-based access has been applied. Organization Name retains all logs online with {Tool} for one (1) year in {Tool}.

## Memory Protection

The information system uses virtual servers running {List Operating Systems}. This operating system {has/does not have} protections in place for preventing code execution in restricted memory locations: No Execute (NX), Address Space Layout Randomization (ASLR), and Data Execution Prevention (DEP).