# System and Information Integrity Procedure

|  |  |  |  |
| --- | --- | --- | --- |
| Procedure Owner |  |  | |
| Procedure Approver(s) |  |
| Effective Date |  | Next Review Date |  |

# Purpose

The purpose of this procedure is to define a consistent approach to manage System and Information Integrity of the IT environment at [COMPANY NAME].

# Scope

This procedure is consistent with CMMC and covers all system and information integrity procedures within [COMPANY NAME] environment. This procedure will be followed by all employees of [COMPANY NAME]. The CMMC System Security Plan (SSP) will be updated to reflect any significant modifications made to this procedure.

# Definitions

**Employees**: All individuals belonging to one or many groups defined below:

1. All individuals associated with [COMPANY NAME] through an employee – employer relationship or contract between [COMPANY NAME] and their employer or [COMPANY NAME] and individual.
2. All individuals possessing equipment issued by [COMPANY NAME]
3. All individuals working on the premises of [COMPANY NAME] and/or utilizing the Internet services provided by [COMPANY NAME].

# Governing Laws, Regulations, and Policies

* NIST SP 800-171, 3.14.1 - 3.14.7
* CMMC SI.L2-3.14.1 – SI.L2-3.14.7
* [COMPANY NAME] – SI – 3.14 - System and Information Integrity Policy

# Procedure Statements

**SI.L1-3.14.1 – Identify, report and correct information and information system flaws in a timely manner:**

1. [COMPANY NAME] conducts a weekly review of Information System in order to Identify any system flaws.
2. On a weekly basis, the <role> reviews vendor sites, bulletins, and notifications to identify potential software/firmware patches related to the Information System(s) under their purview. Additional resources are identified below:

* United States Computer Emergency Readiness Team (US-CERT).
* National Vulnerability Database (NVD).
* Cyber Collaboration Center.
* Microsoft Alerts and Notifications (Windows Operating Systems).
* (Insert Firewall) Firewall Alerts and Notifications (Firewall).
* (Insert AV Tool) Microsoft Defender Alerts and Notifications (Anti-Virus Protection).
* (Insert SIEM Tool) Alerts and Notifications (Security Event Manager).

1. If any system flaws are found in the information system review, the specified time to report system flaws is specified as 24 hours.
2. If system flaws are found by [COMPANY NAME], the <role> will send the system flaw information to the <role>.
3. [COMPANY NAME]’s timeline for correcting system flaws is specified to be completed within 30 days. If system flaws are not feasible to be remediated within 30 days, then the <role> will document the system flaw on the POA&M. The flaw added to the POA&M will be remediated in the most-timely fashion.
4. [COMPANY NAME] <Information Technology department> will work to correct any system flaws within the specified time frame (30 days or by the time specified in the [COMPANY NAME] POA&M).

**SI.L1-3.14.2 – Provide protection from malicious code at appropriate locations within organizational information systems:**

1. The [COMPANY NAME] <System Administrator> manages the malicious code protection mechanisms on the company information system’s under its purview with (Insert AV Tool). All [COMPANY NAME] physical organizational systems have host-based protection that includes AV/Malware/EDR identification and remediation capabilities that report identified issues to the <role> based on criticality level.
2. [COMPANY NAME] ensures that all capable Information System components employ malicious code protection mechanisms to detect and eradicate malicious code. When necessary, the IT staff leverages the publicly available analysis performed by independent organizations (e.g., the FBI, Law Enforcement, vendors, etc.) to gain an understanding of malicious code characteristics and behavior.

**SI.L1-3.14.4** **– Update malicious code protection mechanisms when new releases are available:**

1. [COMPANY NAME] implements (Insert AV Tool) malicious code protection mechanisms that are configured to automatically update upon availability of new updates. These updates are monitored and verified by the <role>.

**SI.L1-3.14.5** – **Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed:**

1. [COMPANY NAME]’s frequency for malicious code scans is set on a weekly schedule to conduct a full scan. This schedule is set by the <role>. All information acquired from (Insert AV Tool) is placed in a centralized management console for administrative review.
2. Malicious code scans are configured to be performed automatically at the weekly defined schedule.
3. The malicious code protection mechanisms are configured by the <role> to conduct real-time malicious code scans of files from external sources as files are downloaded, opened, or executed. The malicious code protection mechanisms then block, quarantine or delete malicious code and alert the <IT staff> via email notifications of malicious code detection.
   * The detection of malicious code is immediately reported to the <role> and the results from associated virus scans are incorporated into the Incident Response and Flaw Remediation processes.
   * When identified, the <role>, or designated representative addresses the receipt of false positives during malicious code detection/eradication and the resulting impact on the availability of the Information System.

**SI.L2-3.14.3** **- Monitor system security alerts and advisories and take action in response:**

1. Response actions are identified in coordination to system security alerts and advisories based on the Risk/Impact and the due care of the <role>.
2. Published system security alerts, notifications, advisories, and directives are monitored through subscribed external resources for review and action, including publications and alerts from:
   * United States Computer Emergency Readiness Team (US-CERT)
   * Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
   * CyberSecurity & Infrastructure Security Agency (CISA)
   * National Vulnerability Database (NVD)
   * Information Sharing and Analysis Centers (ISACs)
   * Cyber Collaboration Center
3. Response actions to system security alerts and advisories are to be implemented within a timely manner, but not to exceed 30 days If the alerts and/or advisories are found to impact the company as deemed by the <role> If the timeline cannot be met, a POA&M is generated and submitted through to the <role>. Any changes to the [COMPANY NAME] security policies, procedures, or processes shall be approved by the <Change Control Board> and communicated to all directly involved parties. Implementation of the changes will occur based on the requisite change management timeline identified in the [COMPANY NAME] Configuration Management Policy.

**SI.L2-3.14.6 – Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks:**

1. The system is monitored to detect attacks and indicators of potential attacks; System level monitoring requirements are reviewed weekly or based on review of intrusion attempt(s). In the event of exploit, the <role> is notified, and the process is governed by the [COMPANY NAME] Incident Response Plan. The tools used are listed below;
2. [COMPANY NAME] employs a variety of automated tools and techniques to accomplish a holistic system monitoring approach to detect attacks and indicators of potential attacks and unauthorized local, network and remote connections which includes, but is not limited to:
   * (Insert Firewall) for boundary protection with gateway protection, intrusion detection capabilities and continuous monitoring of ingress and egress communications traffic for unauthorized activities and conditions.
   * (Insert SIEM Tool) for real-time system audit record monitoring and logging, network monitoring and alerts.
   * Built-in operating system and component auditing capabilities.
   * (Insert AV Tool) for malicious code detection and protection
3. Inbound communications traffic is monitored and audited by the [COMPANY NAME] <IT Department> to detect attacks and indicators of potential attacks. The information is then sent and reviewed by the <role> on a weekly or as needed basis.
4. Outbound communications traffic is monitored and audited by the [COMPANY NAME] <IT Department> to detect attacks and indicators of potential attacks. The information is then sent and reviewed by the <role> on a weekly or as needed basis.

**SI.L2-3.14.7** **– Identify unauthorized use of organizational systems:**

1. Authorized use of the [COMPANY NAME] information system is defined as any appropriately cleared employee with a requirement to access the CUI information system (IS) for performing or assisting in a lawful business-related purpose.
2. (Insert SIEM Tool), (Insert Firewall),and (Insert AV Tool) is deployed to identify unauthorized use of organizational systems and collect essential information in real-time, track specific types of transactions of interest to the company and provide automated alerts. The <IT staff> reviews these audit records on a weekly basis to detect:
   * Attacks and indicators of potential attacks (Indicators of Compromise (IOCs)).
   * Malicious code detection mechanism alerts.
   * Boundary protection mechanism alerts (e.g., firewall alerts).
   * Unauthorized local, network, or remote connections.
   * Unauthorized and/or inappropriate use.
   * Unusual inbound and outbound communications traffic.

**Roles and Responsibilities**

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibilities** | **Contact Information** |
|  |  |  |
|  |  |  |

# Non-Compliance

Violations of this policy will be treated like other allegations of wrongdoing at [COMPANY NAME]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [COMPANY NAME] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
| V.01 | 11/21/2022 | Securestrux | Initial draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |