





A System and Information Integrity Policy defines how an organization can ensure that the data processed by their systems is accurate, complete, and reliable. It is designed to allow organizations to protect the integrity of their data by preventing unauthorized access, modification, or destruction of data whether accidental or malicious. This policy is also meant to help maintain trust in the information used and provided by the organization.

Recommended Actions:

-  Identify and remediate system flaws in a timely manner
-  Implement malicious code protection
-  Perform system and file scanning
-  Monitor system activity for integrity violations

The following template may be used to help with the creation and implementation of your own policies and procedures.

For more information related to System and Information Integrity and other fundamental areas please visit the following link:

[CMMC Assessment Guide Level 1](#)

Policy #:	Title:	Effective Date:
	System and Information Integrity Policy	

PURPOSE

To ensure that Information Technology (IT) resources and information systems are established with system integrity monitoring to include areas of concern such as malware, application and source code flaws, industry supplied alerts and remediation of detected or disclosed integrity issues.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – System and Information Integrity (SI), NIST SP 800-12, NIST SP 800-40, NIST SP 800-45, NIST SP 800-83, NIST SP 800-61, NIST SP800-83, NIST SP 800-92, NIST SP 800-100, NIST SP 800-128, NIST SP 800-137, NIST SP 800-147, NIST SP 800-155

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. FLAW REMEDIATION

IT Department shall:

- a. Identify, report, and correct information system flaws.
- b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
- c. Install security-relevant software and firmware updates within _____ of the release of the updates.
- d. Incorporate flaw remediation into the configuration management process.
- e. Employ automated mechanisms _____ to determine the state of information system components with regard to flaw remediation.

2. MALICIOUS CODE PROTECTION

IT Department shall:

- a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

- b. Update malicious code protection mechanisms whenever new releases are available in accordance with configuration management policy and procedures.
- c. Configure malicious code protection mechanisms to:
 - i. Perform periodic scans of the information system _____ and real-time scans of files from external sources at endpoint; network entry/exit points as the files are downloaded, opened, or executed in accordance with the security policy.
 - ii. Block malicious code; quarantine malicious code; send alert to administrator; _____ in response to malicious code detection.
 - iii. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

1. INFORMATION SYSTEM MONITORING

IT Department shall:

- a. Monitor the information system to detect:
 - i. Attacks and indicators of potential attacks.
 - ii. Unauthorized local, network, and remote connections.
- b. Identify unauthorized use of the information system through defined techniques and methods.
- c. Deploy monitoring devices strategically within the information system to collect _____
and at ad hoc locations within the system to track specific types of transactions of interest to the entity.
- d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
- e. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to operations and assets, individuals, other organizations, or based on law enforcement information, intelligence information, or other credible sources of information.

- f. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable state and federal laws, directives, policies, or regulations.
- g. Provide information system monitoring information to authorized personnel or business units as needed.

2. SYSTEM-GENERATED ALERTS

IT Department shall ensure that:

- a. The information system that may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers will be disseminated to authorized personnel or business units that shall take appropriate action on the alert(s).
- b. Alerts be transmitted telephonically, electronic mail messages, or by text messaging as required. Personnel on the notification list can include system administrators, mission/business owners, system owners, or information system security officers.

3. SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

IT Department shall:

- a. Receive information system security alerts, advisories, and directives from _____ on an ongoing basis.
- b. Generate internal security alerts, advisories, and directives as deemed necessary.
- c. Disseminate security alerts, advisories, and directives to:

- d. Implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

4. SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

IT Department shall:

- a. Employ integrity verification tools to detect unauthorized changes to

- b. Ensure the information system performs an integrity check of

at startup, and/or at

- c. Incorporate the detection of unauthorized _____ into the incident response capability.

5. SPAM PROTECTION

IT Department shall:

- a. Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages.
- b. Update spam protection mechanisms when new releases are available in accordance with the configuration management policy and procedures.
- c. Manage spam protection mechanisms centrally.
- d. Ensure information systems automatically update spam protection mechanisms.

6. INFORMATION INPUT VALIDATION

IT Department shall:

- a. Ensure the information system:
 - i. Checks the validity of _____
 - ii. Provides a manual override capability for input validation of _____
 - iii. Restricts the use of the manual override capability to only _____
 - iv. Audits the use of the manual override capability.
 - v. Reviews and resolve within input validation errors.
 - vi. Behaves in a predictable and documented manner that reflects system objectives when invalid inputs are received.

7. ERROR HANDLING

IT Department shall:

- a. Ensure the information system:
 - i. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.
 - ii. Reveals error messages only to _____.

8. INFORMATION HANDLING AND RETENTION

IT Department shall:

- a. Handle and retain information within the information system and information output from the system in accordance with applicable state and federal laws, directives, policies, regulations, standards, and operational requirements.

9. MEMORY PROTECTION

IT Department shall:

- a. Ensure the information system implements _____ to protect its memory from unauthorized code execution.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	
Date Reviewed:	