|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Policy**:  **System and Information Integrity** | **Updated:** 10/29/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

The System and Information Integrity Policy establishes a framework for maintaining the integrity of IT resources and information systems, focusing on monitoring mechanisms to identify and address integrity issues such as malware, application vulnerabilities, and security alerts. By ensuring proactive detection and remediation of potential threats, the organization aims to safeguard its information assets from unauthorized access and manipulation.

Adopting this policy enhances the organization’s cybersecurity posture by systematically addressing integrity-related concerns. It enables proactive threat management through regular monitoring and prompt remediation of system flaws and vulnerabilities, thereby reducing the risk of breaches. Ensuring the integrity of software and firmware fosters a stable operational environment while aligning with best practices, including the NIST Cybersecurity Framework, to support compliance with legal and regulatory requirements. This policy also promotes a culture of security awareness among all stakeholders, emphasizing the importance of protecting information assets.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Policy Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

The System and Information Integrity Policy applies to all employees, contractors, and third-party vendors interacting with the organization’s information systems and networks. It mandates regular monitoring for unauthorized access, flaw remediation, and protection against malicious code. Key components include ensuring timely identification and correction of system flaws, testing updates before deployment, and implementing mechanisms to detect and eradicate malware at system entry and exit points. Continuous observation of the system for attacks and unauthorized connections is required, along with the protection of sensitive monitoring data. Additionally, the use of integrity verification tools to detect unauthorized changes to critical software and firmware, including periodic integrity checks, is mandated. By following these guidelines, the organization seeks to maintain a secure and resilient information environment, with non-compliance potentially resulting in disciplinary actions to reinforce the critical nature of integrity in safeguarding organizational assets.

* 1. Flaw Remediation

The [Owner] shall:

1. Identify, report, and correct information system flaws.
2. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
3. Install security-relevant software and firmware updates within [entity defined time period] of the release of the updates.
4. Incorporate flaw remediation into the configuration management process.
5. Employ automated mechanisms [entity defined frequency] to determine the state of information system components with regard to flaw remediation.
   1. Malicious Code Protection

The [Owner] shall:

1. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.
2. Update malicious code protection mechanisms whenever new releases are available in accordance with configuration management policy and procedures.
3. Configure malicious code protection mechanisms to:
   1. Perform periodic scans of the information system [entity defined frequency] 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.
   2. Block malicious code; quarantine malicious code; send alert to administrator; [entity defined action] in response to malicious code detection.
   3. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.
   4. Information System Monitoring

The [Owner] shall:

1. Monitor the information system to detect:
   1. Attacks and indicators of potential attacks.
   2. Unauthorized local, network, and remote connections.
2. Identify unauthorized use of the information system through defined techniques and methods.
3. Deploy monitoring devices strategically within the information system to collect [entity determined essential information] and at ad hoc locations within the system to track specific types of transactions of interest to the entity.
4. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
5. 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.
6. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable state and federal laws, directives, policies, or regulations.
7. Provide information system monitoring information to authorized personnel or business units as needed.
   1. System-Generated Alerts

The [Owner] shall ensure that:

1. 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).
2. 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.
   1. Security Alerts, Advisories, and Directives

The [Owner] shall:

1. Receive information system security alerts, advisories, and directives from [entity defined external organizations] on an ongoing basis.
2. Generate internal security alerts, advisories, and directives as deemed necessary.
3. Disseminate security alerts, advisories, and directives to: [entity defined personnel or roles]; [entity defined elements within the organization]; [entity defined external organizations].
4. Implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.
   1. Software, Firmware, and Information Integrity

The [Owner] shall:

1. Employ integrity verification tools to detect unauthorized changes to [entity defined software, firmware, and information];
2. Ensure the information system performs an integrity check of [entity defined software, firmware, and information] at startup, and/or at [entity defined transitional states or security-relevant events], [entity defined frequency].
3. Incorporate the detection of unauthorized [entity defined security-relevant changes to the information system] into the incident response capability.
   1. Spam Protection

The [Owner] shall:

1. Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages.
2. Update spam protection mechanisms when new releases are available in accordance with the configuration management policy and procedures.
3. Manage spam protection mechanisms centrally.
4. Ensure information systems automatically update spam protection mechanisms.
   1. Information Input Validation

The [Owner] shall ensure that the information system:

1. Checks the validity of [entity defined information inputs].
2. Provides a manual override capability for input validation of [entity defined inputs].
3. Restricts the use of the manual override capability to only [entity defined authorized individuals].
4. Audits the use of the manual override capability.
5. Reviews and resolve within input validation errors.
6. Behaves in a predictable and documented manner that reflects system objectives when invalid inputs are received.
   1. Error Handling

The [Owner] shall ensure the information system:

1. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.
2. Reveals error messages only to [entity defined personnel or roles].
   1. Information Handling and Retention

The [Owner] shall 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.

* 1. Memory Protection

The [Owner] shall ensure the information system implements [entity defined security safeguards] to protect its memory from unauthorized code execution.

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
|  |  |

# 8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 10.0 Related Documents

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-40 – Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology](https://csrc.nist.gov/pubs/sp/800/40/r4/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-83 – Guide to Malware Incident Prevention and Handling for Desktops and Laptops](https://csrc.nist.gov/pubs/sp/800/83/r1/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-61 – Computer Security Incident Handling Guide](https://csrc.nist.gov/pubs/sp/800/61/r2/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-92 – Guide to Computer Security Log Management](https://csrc.nist.gov/pubs/sp/800/92/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-128 – Guide for Security-Focused Configuration Management of Information Systems](https://csrc.nist.gov/pubs/sp/800/128/upd1/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-137 – Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations](https://csrc.nist.gov/pubs/sp/800/137/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-147 – BIOS Protection Guidelines](https://csrc.nist.gov/pubs/sp/800/147/final)