Effective: *08/08/2022*
Last Revised: *08/08/2022*

Responsible University Administrator:
Assistant Vice President, IT Security Services

Responsible University Office:
Information Technology Services

Policy Contact:
IT Security Services
security@nebraska.edu

ITS-17: System and Informational Integrity Standard

Standard Contents

1. Purpose

The purpose of the System and Informational Integrity Standard is to define the organization's management of risks pertaining to system flaws/vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling. The standard outlines the methods and requirements for communicating with users about security standards and technological risks.

2. Scope

This standard shall apply to all The University of Nebraska ("The University") technology assets. Any information not specifically identified as the property of other parties, that is transmitted or stored on Information Systems (including email, messages, and files) shall be considered the property of The University and to which this standard applies. All users (employees, contractors, vendors, or others) of Information Systems are responsible for adhering to this standard.

3. Standard Statement

It is the intention of this standard to establish best practices as it pertains to system configuration, error handling, and security. Deviations from the requirements defined herein in the form of exceptions must be approved in advance and in writing by the Chief Information Security Officer ("CISO") as defined in **ITS Policy Exception Standard**. The following subsections outline the System and Information Integrity Standard.

4. System and Informational System Requirements

4.1 Management of Information System Flaws

4.1.1 - Patch Notification
System administration teams for University information systems must subscribe to vendor notifications providing updates about common system problems and vulnerabilities. Procedures must be implemented to periodically review these vendor notices to identify software and firmware updates with security impact.

4.1.2 - Patch Schedules
System administration teams must define patching schedules in coordination with service owners to confirm that information systems and applications are patched to appropriate levels in a timely manner, considering potential production impacts. Patch schedules must be implemented based on asset criticality.

4.1.3 - Patch Analysis
All vendor-released patches must be analyzed by support teams for criticality, applicability, and potential business impact. Patches must be classified based on University-defined criteria.

4.1.4 - Patch Deployment
Reviewed security patches must be deployed to all relevant systems across the environment in alignment with University-defined remediation schedules based on the assigned criticality. Patch application must be tracked across all relevant assets to ensure completeness of patch deployment.

In circumstances in which a vulnerability cannot or will not be remediated in accordance with the defined schedule, the IT Security Services team in conjunction with the team responsible for supporting the Information System must document a business reason and assign compensating controls after evaluating the level of risk.

4.1.5 - Patch Testing
Where possible all patches must be tested in a non-production environment prior to deploying the patch into the production environment, validate the patch will not produce unintended negative security or operational impacts, in alignment with the **Configuration Management Standard.**

4.1.6 Automatic Updates
System updates must be centrally managed by University system administration teams and must not be configured to deploy automatically following release by the vendor unless formally authorized in writing by the CIO or CISO.

4.2 Information System Monitoring and Detection

4.2.1 Information System Monitoring
Security tools and monitoring products must be deployed at the network perimeter, on endpoints, and throughout the network to monitor, identify, and notify University support teams of potential anomalous activity that could impact the confidentiality, integrity, or availability of organization information systems. These may include, but are not limited to:

- Perimeter, network, web application, and host-based firewalls
- Privileged access management solutions
- Intrusion protection / detection systems
- Anti-virus / anti-malware
- Security event logs in accordance with the Audit and Accountability Standard
- Data Loss Prevention solutions
- Rogue device scanning solutions

The level of information asset monitoring activity should be heightened whenever there is an indication of increased risk to organizational operations, assets, individuals, or other organizations based on law enforcement information, intelligence information, or other credible sources of information. The level of monitoring necessary is dependent on the data risk classification of the information system with which the data interacts with.

4.2.2 Threat Detection
A centralized system, such as a Security Information and Event Management System (SIEM) must be established to centrally collect, correlate, and analyze alerts from organizational security appliances, security log files, and monitoring products. This solution must be configured to detect instances of potentially malicious activity, based on defined threat scenarios.

Security analysts must periodically review the coverage of tool monitoring and alerting capabilities against the organizational threat landscape to ensure appropriateness of monitoring coverage. Security analysts must coordinate with security tool owners and system administrators to ensure monitoring rulesets are accurately tuned for event detection. As part of all new system deployments, and before any system goes into production, system administrators must enable appropriate audit logging and coordinate the centralized collection of those logs with the SIEM management team.

4.2.3 Incident Response
All positive alerts detected by University security monitoring solutions must be forwarded to incident response staff for triage and response, in alignment with the Incident Response Standard.

4.2.4 Anti-Virus and Anti-Malware Software
Anti-virus and anti-malware solutions must be implemented on University managed endpoints (e.g., laptops, desktops, mobile devices, and servers) connected to the network and configured to update definitions in a timely manner when they are made available.

Access restrictions must prohibit the disabling of anti-virus and anti-malware solutions by end-users and alerting must be implemented to detect any instances of device non-compliance.

4.2.5 Anti-Virus and Anti-Malware Scans
Anti-virus and Anti-Malware solutions must be configured to detect, quarantine, and eradicate malicious code when it enters the network and at rest. This can be done through implementation of real-time, active scans, and periodic scans.

4.2.6 Spam Protection

Spam protection mechanisms must be implemented at system entry and exit points, at workstations, servers, and mobile computing devices in order to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means. In addition, updates to spam protection mechanisms (including signature definitions) should be administered when new releases are available. Personnel must take all reasonable and appropriate measures to prevent non-public information from being lost, stolen, intercepted, or shared by/with unauthorized individuals. Non-public information may be shared only with:

- Other University employees with authorization to access the information
- Third party vendors approved through University vendor risk management in alignment with services provided, with appropriate contractual provisions in place
- Legally authorized individuals, such as in response to a subpoena or to other entities as required by law

4.3 Email Protections

4.3.1 E-mail Forgery Protections

E-mail protections must be implemented to mitigate malicious or fraudulent messaging. Protection examples include Sender Standard Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC).

4.3.2 Sandboxing

An isolated e-mail sandbox should be leveraged to execute an attached file or linked URL before allowing attachments or links to be opened on the production network. By opening these files or links in a protected environment, the system detects malicious activity before it is introduced into the network.

5. Standards and Procedures

Standards and procedures specific to this policy are to be documented and maintained by the individual affiliates throughout the University system.

6. Compliance

Compliance Measurement

The University of Nebraska Information Security team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be documented and formally approved by the CISO. Standard exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the policy exception is required
- Any risks created by the policy exception
- Risk mitigation plan and duration of the exception
- Evidence of approval by the CISO

Non-Compliance

Failure to comply with University IT standards may result in sanctions relating to the individual's use of IT resources or other appropriate sanctions according to policies applicable to University faculty and staff or student conduct.

7. Related Information

The following is a listing of related Policies, Executive Memoranda, Standards, Controls, and Procedures.

NIST 800-53
NIST 800-171
NU Executive Memorandum 16
NU Executive Memorandum 26

University-Wide Policies & Guidelines - https://nebraska.edu/offices-policies/policies
ITS-00 Information Technology Definitions and Roles
ITS Knowledge Base - https://uofnebraska.sharepoint.com/sites/NU-ITS/KB

8. Approvals and Revision History

Approval of this policy:

	Name	Title	Date
Authored by:	Richard Haugerud	CISO	08/08/2022
Approved by:	Bret Blackman	IT CIO	08/08/2022

Revision history of this policy:

Version	Date	Description
1.0	08/08/2022	Initial Standard Published