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-13: Risk Management Standard

Policy Contents

1. Purpose

The Risk Management Standard defines the organization's requirements for enforcing effective Risk Management control management. The Risk Management Standard will implement strategies to proactively identify threats and vulnerabilities to manage information security risks posed to The University.

2. Scope

The Risk Management 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 a Risk Management capability throughout The University to assist in identifying, assessing, and mitigating information security risk in the environment. 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 Risk Management Standard.

4. Risk Management Requirements

4.1 Risk Appetite

4.1.1 Risk Tolerance

The University must define an information security risk tolerance to guide resource allocation and investments by aligning the organization, people, and processes on how to apply information security practices to effectively identify, detect, protect against, respond to, and recover from information security risks.

Senior management must update this risk tolerance annually to remain current with applicable business changes. This includes changes related to business, legal, cyber threat, regulations, and internal business processes.

4.2 Identify and Evaluate Risk

4.2.1 Risk Assessments

Risk assessment identifies potential risks to an organization's functions and supporting assets: people, technology, information, and facilities. A risk assessment review must be conducted for all applicable business operations (mission, functions, image, or reputation), assets, and individuals on an annual basis or following significant changes to the business environment. The risk assessment review must follow a common methodology to measure the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the information asset and/or the information it processes, stores, or transmits.

Risk exists when threats have an ability to impact the confidentiality, integrity or availability of University assets. Refer to the **Situational Awareness Standard** for additional information regarding threats.

Risk must be assigned to information systems per FIPS PUB 199. This includes an evaluation of risk (low, medium, high) to a system's confidentiality, integrity, or availability. Refer to FIPS PUB 199 for additional information.

Risk assessments should consider the probable frequency (or likelihood) and impact (or magnitude) of losses. Potential forms of loss to consider include but aren't limited to:

- Effort to investigate an event
- Potential disruption due to system / process outages
- Potential fines and judgements related to sensitive data loss
- Loss of intellectual property
- Reputation damage
- Cost of credit monitoring, communications, legal, etc.

4.3 Vulnerability Management

4.3.1 Vulnerability Scanning

Vulnerability scans are required to be performed against University owned assets, including applications, databases, network devices, and operating systems, at defined frequencies based on risk level.

Scanning of the campus network (and all connected devices) and cloud-hosted environments should occur at least quarterly. Scans of the data center should occur every two weeks.

Additionally, the following controls should be defined and maintained:

- Controls to analyze the vulnerability scan reports for false positives (flagging a vulnerability that doesn't exist) and false negatives (scanner missing a valid vulnerability)
- Controls to track the vulnerability remediation by tying it to an incident management ticket and/or a change request

A vulnerability management plan for University systems and applications that are hosted on third-party, or cloud, infrastructures must be established as well as defined dependencies between incident management, change management, configuration management, and patch management processes.

Scans will cover the following types of University IT infrastructure:

- **Network** – Shall mean and include wired and wireless video, voice, and data infrastructure, including security devices (e.g., firewalls, management tools, etc.)
- **Endpoints** – Shall refer to desktops, laptops, tablets, mobile devices, printers, or any other device capable to connecting to the University network.
- **Systems** – Shall mean and include software, servers, storage, licensed platforms, and cloud-based services.
- **Application** – Comprised of University-owned or operated software applications, web applications, etc.

ITS Information Security Services should define and implement an application security program that includes, but is not limited to, the following controls: keeping an application inventory, scanning (both authenticated and unauthenticated) periodically, analyzing, and prioritizing vulnerability, and tracking remediation to closure.

ITS Information Security Services must meet with Infrastructure team monthly to ensure any changes to environments are accounted for and included, as necessary, in upcoming vulnerability scans.

The University **Vulnerability Management Procedure** must have the following defined:

- Frequency for scanning campus network, end-user workstation, IoT devices, and printers
- Standard adopted for rating the severity of the vulnerability
- Remediation timeline based on the severity of the vulnerability
- The baseline for web application scan, for example, Open Web Application Security Project (OWASP) Top 10 and/or SANS (name, no abbreviation available) top 25
- The baseline for a host (servers, end-user systems, printers, more) based scan, for example, Common Weakness Enumeration (CWE) listing and/or the National Vulnerability Database (NVD)
- Metrics to measure the effectiveness of the vulnerability management process.

4.3.2 Vulnerability Remediation or Quarantine

Vulnerabilities identified from scanning, testing, and monitoring activities must be reviewed by University IT Security Services personnel. Vulnerabilities must be prioritized by risk, assigned ownership, and remediated in accordance with established remediation timelines based on vulnerability criticality:

Vulnerability Compliance Timeline		
Severity	Remediation Time Frame	POAM / Quarantine Determination
Urgent (Zero-Day / As-Directed)	7 calendar days	CISO Directed
Critical	15 calendar days	> 30 days
High	30 calendar days	> 60 days
Medium	45 calendar days	> 90 days
Low	60 calendar days	> 120 days

Scans will be performed to verify fixes / patches of discovered vulnerabilities are successful. Only then should the vulnerability be documented as remediated.

A Vulnerability Management Committee will discuss the status of remediation efforts on a weekly basis. An additional steering committee made up of distributed IT staff must meet bi-weekly to identify and formalize mitigation plans for both ITS and non-ITS managed assets.

If the vulnerability scanning software causes a service disruption, the support person shall submit an Exception Request to its-sec@nebraska.edu or create a support ticket. In this case, vulnerability scans will be manually processed. All efforts shall be made and documented to technically remediate the vulnerability.

If the vulnerability cannot be remediated, an exception may be granted. Exceptions must be approved in writing by the Chief Information Security Officer ("CISO") as defined in ITS Policy Exception Standard. The Information Security Office will maintain all documentation regarding inability to fix vulnerabilities and all exception requests.

Where vulnerability remediation cannot be completed within defined remediation timelines, system owners or administrators must complete a Plan of Action and Milestones (POAM) that details the plan and timeline to remediate the vulnerability, implement alternative mitigating controls, and seek a risk acceptance approval. Exceptions should be considered temporary. All exceptions will be reviewed annually for continued approval.

4.3.3 PCI DSS Vulnerability Scanning & Penetration Testing Requirements

Per Payment Card Industry (PCI) Data Security Standard (DSS), the following must occur for cardholder data environments (CDEs) if required by the Payment Card Industry (PCI) Data Security Standard (DSS):

- All outward facing IP addresses and domains exposed in the CDE are to be scanned by a PCI Approved Scanning Vendor (ASV) at least quarterly
- Internal and external vulnerability scanning must be performed:
    - An internal scan is performed within the network perimeter
    - An external scan is performed outside of the network in order to identify known weakness in network infrastructure
- Internal and external penetration testing should occur at least annually of the network and application layers of the CDE
- Vulnerability scans and penetration tests should occur if there is a significant change to the CDE. Examples of significant changes are:
    - OS upgrade for CDE system
    - Replacing firewall or critical security device
    - Adding a new payment acceptance process
    - Moving portions or all of the environment to a cloud-hosted environment

4.4 Third Party Risk Management

4.4.1 Vendor Due Diligence

A Vendor Risk Assessment will be conducted before The University undertakes any activities with a vendor that involves processing of high-risk data or access to IT systems. Vendor Risk Assessments must:

- Identify services/solutions to be provided by the vendor, based on the proposed scope of work, that require access to high-risk data and IT systems
- Document reasonably foreseeable internal and external risks to security, data and privacy posed by the vendor and its services/solutions
- Provide recommendations to remediate or mitigate risks
- Verify capabilities of the vendor to ensure their ability to deliver their services/solutions in compliance with University data security and privacy requirements
- Verify vendor compliance with legal and regulatory obligations
- Ensure the vendor is meeting all requirements of the CMMC compliance
- Verify vendors are meeting service level agreements and contractual obligations
- Approval of vendor agreements by the CIO and/or CISO

4.4.2 Vendor Performance Monitoring

Ongoing oversight, including periodic re-assessment of vendor due diligence, must be maintained on vendors processing University high-risk data or having access to University systems to confirm vendor performance meets contract terms, including implementation of any remediation actions. Processes must be defined and implemented for monitoring the vulnerability management processes of the University's hosting and service providers.

4.5 End of Life Asset Management

4.5.1 Management of Non-vendor Supported Products

IT support teams must periodically review the IT environment for assets that will no longer be supported by the vendor. For assets in production that will no longer be supported, IT support teams must remove these assets from production environments, replace or upgrade them to a newer supported version, or develop roadmaps detailing mitigation plans for these assets. Mitigation plans must be approved by the CISO for appropriateness, and may include:

- Purchase of extended support from the vendor
- Isolation of unsupported products
- Implementation of system upgrade, replacement, or retirement

4.6 Risk Response and Reporting

4.6.1 Risk Documentation and Classification

Risks identified through assessment activities must be formally documented and assigned ownership within an organizational risk register. Risks must be classified in accordance with criteria established in the Information Security Risk Appetite Statement based on their business impact and residual risk level.

4.6.2 Risk Response

Risk owners must develop risk response plans to determine the appropriate course of action for the identified risk in consideration of business impact, residual risk, and risk appetite. The selected response and supporting management plan must be approved by the CISO based on risk level. These plans must include:

- The proposed response type (avoid, accept, transfer, or mitigate)
- Risk owner provides detailed POAM to mitigate the identified risk, as applicable
- Resources and staff responsible to carry out plan

4.6.3 Risk Reporting
Risk metrics must be aggregated and reported to senior management on a periodic basis to communicate the overall risk exposure to the organization. Accepted risks must be reviewed and reapproved annually to ensure ongoing business justification and appropriateness against enterprise risk appetite.

5. Procedures

Procedures specific to this Standard are to be documented and maintained by the individual service owners throughout the University system.

6. Compliance

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

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

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

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 policies.

7. Related Information

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

NIST 800-53
NIST 800-171
FIPS PUB 199
NU Executive Memorandum 16
NU Executive Memorandum 26
NU Executive Memorandum 41
NU Executive Memorandum 42

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 Standard:

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

Revision history of this Standard:

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