University of Nebraska
LINCOLN | OMAHA | KEARNEY | MEDICAL CENTER

Effective: 12/31/17
Last Revised: 8/28/17

Responsible University Administrator:
Vice Chancellor for Information Services & CIO

Responsible University Office:
Information Technology Services

Policy Contact:
Chief Information Security Officer,
security@nebraska.edu

ITS-04 Vulnerability Management Policy

Scope

This policy governs the University of Nebraska and applies to everyone who conducts work at or provides services to the University or utilizes University information assets, including all faculty, staff, students, contractors, consultants.

Policy Statement

All servers, websites, and applications developed with university resources as defined in Executive Memorandum 16 will be subject to inventory, scanning and security review. All scanning and security review will be conducted under the supervision of the Information Security Office. Under no circumstances will any server, website or application using university resources be allowed to access the network with having first been inventoried, scanned and reviewed.

The University of Nebraska will proactively utilize a vulnerability scanning tool to identify potential security risks to the network, servers and endpoints. It is the goal to mitigate all identified vulnerabilities. In the instance where the technical fixing of the vulnerability presents a greater business risk than the vulnerability, the Exception Process shall be followed.

A. All scanning and security review will be conducted under the supervision of the Information Security Office.

B. All websites, applications or systems that:

C. Work with high and medium risk data as defined the ITS-05 Data Classification and Management Policy.

D. Increase the risk to the University brand(s) through direct brand association.

E. Are developed for a fee using university resources.

F. Put other systems at risk over the network.

G. Jeopardize the safety of people will be subject to inventory, scanning and security review.

Experimental or exploratory sites are not subject to this process unless they are hosted on the university's network or servers.

Reason for Policy

To protect all digital assets and systems at the University of Nebraska from unauthorized access security audits and vulnerability management will be utilized by the University of Nebraska to:

A. Discover and prioritize all networked assets

B. Proactively identify and fix security vulnerabilities

C. Manage and reduce business risk

D. Ensure compliance with laws, regulations and best security practices

Procedures

A. **Vulnerability Scanning Schedule**: The campus network (and all devices that are connected) is scanned periodically to ensure a rotation that will scan all devices. The Data Centers are scanned every two weeks. NOTE: Scans of individual devices by the Information Security Office are viewed as normal trouble shooting and will not be communicated in advance.

1. **Servers:**

1.a. Each system administrator shall have access to the data from the scan for their individual systems.

1.b. The system administrator shall evaluate the results of the scans at a minimum monthly and fix vulnerabilities based upon their professional judgment.

2. **End User Devices (Workstations/Printers etc.)**:

2.a. End User devices (Workstations/Printers) are in scope for the Vulnerability Management Program.

2.b. The support person is responsible for ensuring the devices are fully patched.

2.c. All devices need to have the most current firmware installed.

2.d. All drivers that are installed on the end user devices need to be maintained.

2.e. If the device is experiencing difficulty when being scanned (i.e. network connectivity is lost, printing of random characters etc.), and the firmware and all drivers are up to date, a case will be opened with the vendor.

2.f. Each support person shall have access to the data from the scans.

2.g. The support person shall fix vulnerabilities monthly.

2.h. In the case where a vulnerability cannot be mitigated, the Exception Process shall be followed.

3. **General**

3.a. If a particular device is reporting a large number of open vulnerabilities which is putting the network at risk, the device will be removed from the network

3.b. If a vulnerability cannot be fixed, the support person shall follow the Exception Process and provide written documentation relating to the remediation plan.

4. **Exception Process**

4.a. If the vulnerability scanning software causes the machine to fail, the support person shall submit an Exception Request to security@nebraska.edu

4.b. All efforts shall be made to technically remediate the vulnerability. However, if the vulnerability cannot be remediated, an exception request will be granted

4.c. Disagreements will be escalated to the NU Security Council.

4.d. The Information Security Office will maintain all documentation regarding inability to fix vulnerabilities and all exception requests

5. **PCI Vulnerability Reports**

5.a. The Information Security Office will be responsible for submitting PCI vulnerability reports to the merchant banks in compliance with the PCI regulations in coordination with a campus PCI representative.

B. **Vulnerability Management**

1. Systems working with University high risk data or that serve mission-critical computing purposes must be remediated and mitigation of any detected vulnerabilities will be either in accordance with the Remediation and Mitigation standards below or must have a documented approved exception.

2. The priority of patching or mitigating vulnerabilities based on the severity level given in the scoring process. Remediation must occur within the time frames specified below for each level of severity:

Severity	**Remediation Time Frame**

Urgent	7 days
Critical	15 days
High	60 days
Medium	TBD
Low	TBD

2. Definitions

2.A. **Vulnerabilities**: Threat to the system or digital environment caused by software errors which can be mitigated by patching

2.B. **Vulnerability Management**: Remediation, mitigation, or acceptance associated risks of discovered vulnerabilities.

2.C. **Support Person**: This is the individual who is responsible for supporting/maintaining the device (workstations, server, printer, etc.)

Additional Contacts

Subject	Contact	Phone	Email

Related Information

Executive Memorandum 16

Executive Memorandum 26

ISO 27002

NIST-800-53

History

0.1 First draft created by Matt Morton

0.2 Edited by Matt Morton