Effective: *Date*
Last Revised: *Date*

Responsible University Administrator:
Chief Information Security Officer

Responsible University Office:
Office of Information Security

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

UNIVERSITY OF Nebraska
LINCOLN | OMAHA | KEARNEY | MEDICAL CENTER

POLICY CONTENTS

Security
Vulnerability Management (ITS-04)

Scope

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

Policy Statement

All servers, websites, and applications developed with University resources, and university owned end user devices as defined in Executive Memorandum 16 will be subject to inventory, scanning and security review. All scanning and security reviews 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 University network without having first been inventoried, scanned and reviewed.

The University will proactively utilize a vulnerability scanning tool to identify potential security risks to the network, servers and endpoints. The goal is 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.

All scanning and security review will be conducted under the supervision of the Information Security Office.
All websites, applications or systems that:

- Work with high and medium risk data as defined the ITS-05 Data Classification and Management Policy.
- Increase the risk to the University brand(s) through direct brand association.
- Are developed for a fee using university resources.
- Put other systems at risk over the network.
- 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:

- Discover and prioritize all networked assets
- Proactively identify and fix security vulnerabilities
- Manage and reduce business risk

- Ensure compliance with laws, regulations and security best practices in the NIST family of information security controls (800-53, 800-171, CSF).

Procedures

Vulnerability Scanning Schedule: The campus network, including all connected devices such as end user workstations and printers, is scanned periodically. The Data Centers are scanned at least 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. Each system administrator shall have access to the data from any scan of their individual systems.
    2. The system administrator shall evaluate the results of any scans at least monthly and correct vulnerabilities based upon their professional judgment.
    3. In the case where a vulnerability cannot be mitigated, the Exception Process shall be followed.
2. **End User Devices (Workstations/Printers etc.)**:
    1. The support person is responsible for ensuring the devices are regularly patched.
    2. Endpoints containing high risk data as defined by the High Risk Data and Minimum Security Standards Policy will comply with the standards in that policy.
    3. All devices need to have the most current firmware installed.
    4. All drivers that are installed on the end user devices need to be maintained.
    5. 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.
    6. Each support person shall have access to the data from the scans.
    7. The support person shall correct vulnerabilities at least monthly.
    8. In the case where a vulnerability cannot be mitigated, the Exception Process shall be followed.
3. **General**
    1. 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 without notification.
    2. 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**
    1. If the vulnerability scanning software causes the server, application or end user device to fail, the system administrator or support person shall submit an Exception Request to security@nebraska.edu
    2. All efforts shall be made to technically remediate the vulnerability. However, if the vulnerability cannot be remediated, an exception request will be granted if other technical controls can mitigate the risk
    3. Disagreements will be escalated to the University CISO
    4. The Information Security Office will maintain all documentation regarding inability to fix vulnerabilities and all exception requests and their disposition
5. **PCI Vulnerability Reports**
    1. 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.

Vulnerability Management
Systems containing 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.
The priority of patching or mitigating vulnerabilities is based on the severity level given in the scoring process. Remediation must occur within the time frames specified in the High Risk Data Definitions and Minimum Data Security Standards or the assets will be subject to removal from the network without notification.

Definitions

Support Person: This is the individual who is responsible for supporting/maintaining the device (workstations, server, printer, etc.) or the employee using the system if there is no support person.

System Administrator: The individual who supports a multi-user computing environment and ensures continuous, optimal performance of IT services and support systems.

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

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

Additional Contacts

Subject	***Contact***	***Phone***	***Email***

Related Information

Executive Memorandum 16
Executive Memorandum 26
NIST-800-53

History

0.1 First draft created by Matt Morton
0.2 Edited by Matt Morton
0.3 Edited by Andrea Childress