VULNERABILITY AND PATCH MANAGEMENT

POLICY NUMBER: ADM-VULNERPATCHMGMT
POLICY TYPE: ADMINISTRATIVE
RESPONSIBLE OFFICIAL TITLE: VICE PRESIDENT-ADMINISTRATION & FINANCE/CFO
RESPONSIBLE OFFICE: INFO. TECHNOLOGY (IT)/CHIEF INFORMATION OFFICER (CIO)
EFFECTIVE DATE: UPON PRESIDENTIAL APPROVAL – 12/12/2023
NEXT REVIEW DATE: PRESIDENTIAL APPROVAL PLUS FOUR (4) YEARS – 12/12/2027
SUPERSEDES POLICY DATED: N/A – NEW POLICY
BOARD OF REGENTS REPORTING (CHECK ONE):
☐ PRESIDENTIAL RECOMMENDATION (CONSENT AGENDA/VOTING ITEM):
☒ PRESIDENTIAL REPORT (INFORMATION ONLY)

I. POLICY STATEMENT

Vulnerability and patch management are essential components of any information security program and vital to effective management of information systems and reduction of associated risk to the university. Vulnerability assessments are used as a means of identifying assets connected to the university's network and the weaknesses associated with them, as well as assessing the risk of those weaknesses. After vulnerabilities are identified, the next step is to address them. Northern Kentucky University (NKU) strives to continually improve its security posture by identifying and remediating vulnerabilities.

All university-owned or operated computer systems and devices must be protected through the timely deployment and installation of software updates, patches, service packs, hot fixes, and signatures. Data Custodians (see sections III and IV below) are responsible for monitoring the latest update releases, applying them on a regular schedule (at least quarterly), and checking to ensure the completeness and effectiveness of their patching processes. All university information systems, devices, and applications must be maintained according to manufacturer recommendations or follow a university-approved maintenance schedule; this includes using only supported operating systems and applications. End-of-life operating systems and applications must be removed before the end-of-life date. Any device not meeting these security standards may be removed from university resources.

The NKU IT Information Security Team will conduct vulnerability assessments of university systems. Targeted vulnerability assessments may also be implemented on an as-needed basis, determined and administered exclusively by the IT Information Security Team or an authorized entity. The university's vulnerability assessment system will be utilized and administered by the IT Information Security Team.

NKU classifies vulnerabilities as follows (see section III below for definitions):

- Catastrophic
- High
- Moderate
- Low
- Informational

All steps must be taken to ensure the proper installation of patches and/or remediation of vulnerabilities. This includes rebooting, registry edits, and uninstalling applications and/or services as recommended.

All security patches must be installed unless testing against critical systems results in system instability or reduction in essential functionality. Exceptions must be documented and a plan to eliminate the exception must be implemented. The IT Information Security Team reserves the right to consider any security patches critical and request immediate installation.

Prior to the implementation of a new system or major change in an existing system on NKU's network, Data Custodians must perform a vulnerability scan using a vulnerability scanner approved by the IT Information Security Team. Data Custodians must remediate any vulnerabilities discovered and maintain proof of remediation.

Data Custodians and/or System Owners must allow access to the university vulnerability management agent or allow for the ability to run authenticated vulnerability scans. Use of any other network-based tools to scan or verify vulnerabilities must be approved in advance by the IT Information Security Team. Once vulnerability assessments have been conducted, the IT Information Security Team will communicate to Data Custodians. It is the responsibility of Data Custodians to cooperate fully with any vulnerability assessment being conducted on systems for which they are accountable.

The Office of Information Security may engage with third parties to conduct internal or external vulnerability assessments or penetration testing as necessary. The IT Information Security Team reserves the right to remove or isolate vulnerable assets from the university's network at any time without prior communication. Once the cyber threat is contained, the Security Team will work with the Data Custodians to seek a resolution.

Any exceptions to this policy for end-of-life operating systems/applications, catastrophic or high-level vulnerabilities must be documented by an approved *Risk Acceptance Form (RAF)* on file with the Office of Information Technology's Security Team. Additional mitigating controls may be required where appropriate.

II. ENTITIES AFFECTED

All faculty, staff, administrators, students, vendors, alumni, and community who utilize the NKU network.

III. DEFINITIONS

NKU classifies vulnerabilities as follows:

- **Catastrophic**: Out-of-band catastrophic vulnerabilities as deemed by the Office of Information Security or university leadership must be remediated as soon as possible, but no later than 7 days. Due to the extremely critical nature these vulnerabilities, exemptions are not available without executive leadership approval and documentation.
- **High (Level 4-5):** High level vulnerabilities must be remediated as soon as reasonably possible, but no later than 30 days after release.
- **Moderate (Level 3):** Moderate level vulnerabilities must be remediated as soon as reasonably possible, but no later than 60 days after release.

- **Low (Level 2):** Low level vulnerabilities must be remediated as soon as reasonably possible, but no later than 90 days after release.
- **Informational (Level 1):** Informational vulnerabilities are often deviations from industry best practice and when possible, should be remediated within 180 days.
- **Data Custodian:** Computer system administrators responsible for the operation and management of systems and servers that store or provide access to institutional data. Data Custodians are typically IT Technical staff; however, they may be faculty or staff who purchase specialized hardware or software through funding sources such as grants or department funding. IT technical staff are not always aware of these specialized items; thus, the purchaser must be responsible for applying updates and patches or submitting a service request for IT technical assistance.
- **System Owner:** The person or organization having responsibility for the development, procurement, integration, modification, operation, maintenance, and/or final disposition of an information system. The system owner is typically IT; however, it may be a faculty or staff member who uses specialized non-standard hardware or software.
- **Vulnerability Remediation:** The process of mitigating or reducing identified vulnerabilities on a system to bring the overall risk associated with that asset down to an acceptable level.

IV. RESPONSIBILITIES

Information Technology (IT) Information Security Team is responsible for conducting vulnerability assessments of university systems. Targeted vulnerability assessments may also be implemented on an as-needed basis, determined and administered exclusively by the IT Information Security Team or an authorized entity. The university's vulnerability assessment system will be utilized and administered by the IT Information Security Team.

Data Custodians are responsible for monitoring the latest update releases, applying them on a regular schedule (at least quarterly), and checking to ensure the completeness and effectiveness of their patching processes.

V. EXCEPTIONS

Exceptions must be documented with NKU's IT Information Security Team and a plan to eliminate the exception must be implemented.

VI. REFERENCES AND RELATED MATERIALS

REFERENCES & FORMS

Risk Acceptance Form

RELATED POLICIES

Risk Acceptance – Information Security *(proposed new policy – will link when available)*

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
New policy	December 12, 2023

VULNERABILITY AND PATCH MANAGEMENT

PRESIDENTIAL APPROVAL

PRESIDENT

Signature Cady Short-Thompson Date 12/12/2023

Cady Short-Thompson

BOARD OF REGENTS APPROVAL

BOARD OF REGENTS (IF FORWARDED BY PRESIDENT)

☒ This policy was forwarded to the Board of Regents on the ***Presidential Report (information only)***.
Date of Board of Regents meeting at which this policy was reported: 1/17/24.

☐ This policy was forwarded to the Board of Regents as a ***Presidential Recommendation (consent agenda/voting item)***.

- ☐ The Board of Regents approved this policy on _____/_____/_____.
  (Attach a copy of Board of Regents meeting minutes showing approval of policy.)
- ☐ The Board of Regents rejected this policy on _____/_____/_____.
  (Attach a copy of Board of Regents meeting minutes showing rejection of policy.)

SECRETARY TO THE BOARD OF REGENTS

Signature Tammy Knochelmann Date 1/18/24

Tammy Knochelmann