Vulnerability Management Policy, version 1.0.0

Status: ☐ Working Draft ☒ Approved ☒ Adopted
Document Owner: Information Security Committee
Last Review Date: November 2024

Vulnerability Management Policy

Purpose

The purpose of the Nebraska Indian Community College (NICC) Vulnerability Management Policy is to establish the rules for the review, evaluation, application, and verification of system updates to mitigate vulnerabilities in the IT environment and the risks associated with them.

Audience

The NICC Vulnerability Management Policy applies to individuals who are responsible for **Information Resource** management.

Contents

Policy

Endpoint Protection (Anti-Virus & Malware)

- All NICC owned and/or managed **Information Resources** must use the NICC IT management approved endpoint protection software and configuration.
- All non-NICC owned workstations and laptops must use NICC IT management approved endpoint protection software and configuration, prior to any connection to a NICC **Information Resource**.
- The endpoint protection software must not be altered, bypassed, or disabled.
- Each email gateway must utilize NICC IT management approved email virus protection software and must adhere to the NICC rules for the setup and use of this software, which includes, but is not limited to, scanning of all inbound and outbound emails.
- Controls to prevent or detect the use of known or suspected malicious websites must be implemented.
- All files received over networks or from any external storage device must be scanned for malware before use.
- Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to NICC IT Support.

Logging & Alerting

- Documented baseline configurations for **Information Resources** must include log settings to record actions that may affect, or are relevant to, information security.
- Event logs must be produced based on the NICC Logging Standard and sent to a central log management solution.
- A review of log files must be conducted periodically.

- All exceptions and anomalies identified during the log file reviews must be documented and reviewed.
- NICC will use file integrity monitoring or change detection software on logs and critical files to alert personnel to unauthorized modification.
- Log files must be protected from tampering or unauthorized access.
- All servers and network equipment must retrieve time information from a single reference time source on a regular basis so that timestamps in logs are consistent.
- All log files must be maintained for at least one year.

Patch Management

- The NICC IT team maintains overall responsibility for patch management implementation, operations, and procedures.
- All **Information Resources** must be scanned on a regular basis to identify missing updates.
- All missing software updates must be evaluated according to the risk they pose to NICC.
- Missing software updates that pose an unacceptable risk to NICC **Information Resources** must be implemented within a time period that is commensurate with the risk as determined by the NICC Vulnerability Management Standard.
- Software updates and configuration changes applied to **Information Resources** must be tested prior to widespread implementation and must be implemented in accordance with the NICC Change Control Policy.
- Verification of successful software update deployment will be conducted within a reasonable time period as defined in the NICC Vulnerability Management Standard.

Penetration Testing

- **Penetration testing** of the internal network, external network, and hosted applications must be conducted at least annually or after any significant changes to the environment.
- Any exploitable vulnerabilities found during a **penetration test** will be corrected and re-tested to verify the vulnerability was corrected.

Vulnerability Scanning

- **Vulnerability scans** of the internal and external network must be conducted at least semi-annually or after any significant change to the network.
- Failed **vulnerability scan** results rated at Critical or High will be remediated and re-scanned until all Critical and High risks are resolved.
- Any evidence of a compromised or exploited **Information Resource** found during **vulnerability scanning** must be reported to the NICC Information Security Officer and IT support.
- Upon identification of new vulnerability issues, configuration standards will be updated accordingly.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 12, 18
- NIST CSF: PR.IP, PR.PT, DE.AE, DE.CM, RS.MI
- Incident Management Policy
- Change Control Policy

- Logging Standard
- Vulnerability Management Standard

Waivers

Waivers from certain policy provisions may be sought following the NICC Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	October 2023			Document Origination
		3-28-2024	IT Committee	Review and Approved
		4-23-2024	Administrative Council	Review and Approved
		6-21-2024	Academic Council	Review and Approved
		8-7-2024	Executive Council	Review and Approved
		11-9-2024	Board of Directors	Review and Approved