Network Management Policy, version 1.0.0

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

Network Management Policy

Purpose

The purpose of the Nebraska Indian Community College (NICC) Network Management Policy is to establish the rules for the maintenance, expansion, and use of the network infrastructure.

Audience

The NICC Network Management Policy applies to individuals who are involved in the configuration, maintenance, or expansion of the NICC network infrastructure.

Contents

Policy

General

- NICC IT owns and is responsible for the NICC network infrastructure and will continue to manage further developments and enhancements to the infrastructure.
- To provide a consistent network infrastructure capable of leveraging new networking developments, all cabling must be installed by NICC IT or an approved contractor.
- **Information security** requirements must be included in any new information system or enhancements to the existing system.
- Appropriate **technical controls** and solutions must be implemented to protect Confidential information from unauthorized transfer, modification, or disclosure (i.e. next-gen firewalls, IDS/IPS, DLP).
- A map or diagram of the network and data flow, including external connections, must be maintained. This map or diagram must be updated after any changes to the network occur. This diagram should be reviewed every 6 months to ensure it continues to represent the network architecture
- All systems on the network must be authenticated. Connections to the network must be authorized by IT.
- All hardware connected to the NICC network is subject to NICC IT management and monitoring standards.
- Documented baseline configurations must be maintained for all **Information Resources** that create, collect, store, and/or process **confidential** or **internal information** and all network connected resources must be configured to these specifications.
- Operating procedures for activities associated with information processing must be documented and made available to personnel who need access to them.
- Resource usage must be monitored to ensure the required system performance.

- Information processing facilities must address redundancy sufficient to meet availability requirements.
- Changes to the configuration of active network management devices must be made according to the Change Control Policy.
- The NICC network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by NICC IT Management.
- All connections of the network infrastructure to external third-party networks are the responsibility of NICC IT.
- Groups of information services, users and information systems must be segregated on the network. The perimeter of each domain should be well defined and based on the relevant security requirements.
- Network devices must be installed and configured following NICC implementation standards.
- The use of departmental network devices is not permitted without the written authorization from NICC IT Management.
- Personnel are not permitted to access or alter existing network hardware in any way.

Wireless Networking

- All wireless access points or devices that provide access to the NICC wireless network must be approved by management.
- Wireless access points must be placed in secure locations.
- Wireless networks must be segmented using appropriate **technical controls**.
- Authentication settings (passwords, encryption keys, etc.) must be changed on a periodic basis as well as anytime it is suspected that such information has been compromised or if anyone with knowledge of the information leaves the organization.
- All wireless network traffic must be encrypted in accordance with the NICC Encryption Policy and supporting standards, regardless of information sensitivity.
- The NICC Wireless Network must not be used inappropriately; in particular, persons must not use the network to:
    - Intercept or attempt to intercept other wireless transmissions for the purposes of eavesdropping.
    - Access or run utilities or services which might negatively impact on the overall performance of the network or deny access to the network, e.g. RF jamming, Denial of Service (DoS).
- NICC wireless network users must not tamper with network access points or security settings.
- Users must not connect to another wireless network and the NICC wireless network simultaneously.
- NICC will conduct scans of wireless access points and identify all authorized and unauthorized wireless access points at least quarterly.

Network Cabling

- Core and distribution racks must be secured and not located in visible areas.
- All networking cabling must be protected from unauthorized interception, organized, tied down and labeled.
- All network closets must be secured with auditable controls.
- Demarcation points need to be secured with adequate segregation or isolation.
- All ports on switches must be reconciled and inventoried regularly. Where this is not possible, compensating controls must be used and documented.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 6, 9, 11, 12, 13, 17
- NIST CSF: PR.AC, PR.DS, PR.IP, PR.PT, DE.CM
- Change Control Policy
- Vulnerability Management Policy
- Asset Management Policy
- Identity and Access Management Policy
- Encryption Policy
- Encryption 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	November 2023		FRSecure	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