Auditing Policy, version 1.0.0

Status: ☐ Working Draft ☒ Approved ☒ Adopted
Document Owner: Information Security Committee
Last Review Date: March 2025

Auditing Policy

Purpose

The purpose of the Nebraska Indian Community College (NICC) Auditing Policy is to establish the requirements for conducting audit-related reviews of information security-resources at NICC.

Audience

The NICC Auditing Policy applies to any individual or process that participates in NICC Information Security audits in any tangible manner.

Policy

- All **information resources** that create, collect, store, and/or process **confidential information** must be audited on a regular basis, according to a documented schedule.
- The scope and conduct of information resource audits must be done in accordance with documented standards and/or procedures.
- System security audits must be led by information security personnel with the specialized training necessary to conduct such audits.
- Personnel conducting system security audits should communicate the following information to information resource owners, custodians, and users, prior to conducting an audit:
    - The date in which the audit will begin,
    - The date in which the audit will end,
    - The scope of the audit,
    - The purpose of the audit,
    - The potential, even if slight, of service disruption.
- **Information resource owners and custodians** must provide reasonable access to information resources in order for audit personnel to conduct security audits in accordance with the documented purpose and scope of the audit.
- All pertinent security audit activities and results must be documented.
- Every security audit deficiency must be accompanied with a recommendation.
- Audit summary reports must be created for each system security audit conducted, and the reports must be provided to management at the conclusion of the audit.
    - The security of exchanges of information are the subject of policy development and compliance audits.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 12.7.1, 18.2.3
- NIST CSF: PR.IP, DE.DP

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	December 2023		FRSecure	Document Origination
		6-25-2024	IT Committee	
		10-25-2024	Academic Committee	Reviewed and Approved
		12-18-2024	Administrative Committee	Reviewed and Approved.
		01-22-2025	Executive Committee	Review and Approved.
		03-29-2025	Board of Directors	Review and Approved.