Risk Management Policy, version 1.0.0

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

Risk Management Policy

Purpose

The purpose of the Nebraska Indian Community College (NICC) Risk Management Policy is to establish the requirements for the assessment and treatment of information security-related risks facing NICC.

Audience

The NICC Risk Management Policy applies to all NICC individuals that are responsible for management, implementation, or treatment of risk activity.

Policy

- Formal organization-wide risk assessments will be conducted by NICC no less than annually or upon significant changes to the NICC environment.
- Risk assessments must account for administrative, physical, and technical risks.
- Information security risk management procedures must be developed and include the following (at a minimum):
    - Risk Assessment
    - Risk Treatment
    - Risk Communication
    - Risk Monitoring and Review
- Risk evaluation criteria should be developed for evaluating the organization's information security risks considering the following:
    - The strategic value of the business information process.
    - The criticality of the information assets involved.
    - Legal and regulatory requirements, and contractual obligations.
    - Operational and business importance of availability, confidentiality, and integrity.
    - Stakeholders expectations and perceptions, and negative consequences for goodwill and reputation.
- All risks will be classified and prioritized according to their importance to the organization.
- Periodically, NICC may contract with a third-party vendor to conduct an independent risk assessment and/or to validate the effectiveness of the NICC risk management process.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 18
    - NIST CSF: ID.GV, ID.RA, ID.RM, PR. IP

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