Personnel Security and Awareness Training Policy, version 1.0.0

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

Personnel Security and Awareness Training Policy

Purpose

The purpose of the Nebraska Indian Community College (NICC) Personnel Security and Awareness Training Policy is to ensure that all personnel with access to NICC **Information Resources** are adequately vetted, qualified, and trained according to their role.

Audience

The NICC Personnel Security and Awareness Training Policy applies to all individuals responsible for hiring, onboarding, offboarding, and training of personnel given access to NICC **Information Resources**.

Contents

Policy

General

- For all roles within NICC, the hiring process should ensure the candidate has the necessary competence to perform the role and can be trusted to take on the role, especially for roles related to the use, management or protection of information security.
- Information security responsibilities must be communicated to employees as part of the on-boarding process.
- All employees are required to sign a Confidentiality/Non-Disclosure Agreement before being granted access to any information resource.
- Upon termination of employment, personnel must be reminded of confidentiality and non-disclosure requirements.
- NICC will provide all employees an anonymous process for reporting violations of information security policies or procedures.

Background Checks

- Background checks are required prior to employing NICC employees, regardless of if a competitive recruitment process is used.
- Background checks may be required for employees who change positions in the company, obtaining more sensitive duties, as determined by Human Resources or the hiring manager.
- Background checks may be required for employees at any time after the employment start date, at the discretion of Human Resources or Executive Management.
- Contractors with access to NICC **confidential information** must have a process in place for conducting background checks on applicable staff. An agreement must be put in place

specifying the responsibilities for conducting background checks if a procedure is not currently being followed or in question.

Training and Awareness

- All new personnel must complete an approved **Security Awareness** training prior to, or within 30 days of, being granted access to any NICC **Information Resources**.
- All personnel, including third parties and contractors must be provided with relevant information security policies to allow them to properly protect NICC **Information Resources**.
- All personnel, including third parties and contractors, must acknowledge they have received and agree to adhere to the NICC Information Security Policies before they are granted to access to NICC **Information Resources**.
- All personnel must complete the annual security awareness training.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 7, 13
- NIST CSF: PR.AT, PR.IP, DE.CM
- Information Security Policy
- Confidentiality/Non-Disclosure Agreement

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
		5-7-2024	IT Committee	Review and Approve
		7-18-2024	Academic	Review and Approve
		8-21-2024	Administrative	Review and Approve
		12-4-2024	Executive Council	Review and Approved
		11-9-2024	Board of Directors	Review and Approved