Vendor Management Policy, version 1.0.0

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

Vendor Management Policy

Purpose

The purpose of the Nebraska Indian Community College (NICC) Vendor Management Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to NICC, its business partners, and its stakeholders from any of its vendors.

Audience

The NICC Vendor Management Policy applies to any individuals that interacts, set up or manage any NICC vendors.

Contents

Policy

Assessments

- Vendors granted access to NICC **Information Resources** must sign the NICC Vendor Non-Disclosure Agreement/Business Associate Agreement.
- Vendors must be evaluated prior to the start of any service and thereafter on an annual basis.
- High risk findings must be followed up to verify remediation.
- A vendor risk assessment must be performed on vendors with physical or logical access to confidential information or that are considered critical vendors.
- Risk assessments must be performed on all requested cloud providers before approval.
- Vendors with PCI DSS compliance requirements must have their status reviewed on an annual basis.

Management

- Vendor agreements and contracts must specify:
  - The NICC information the vendor should have access to,
  - How NICC information is to be protected by the vendor,
  - How NICC information is to be transferred between NICC and the vendor,
  - Acceptable methods for the return, destruction or disposal of NICC information in the vendor's possession at the end of the contract,
  - Minimum information security requirements,
  - Incident response requirements,
  - Right for NICC to audit vendor.

- If a vendor subcontracts part of the information and communication technology service provided to NICC, the vendor is required to ensure appropriate information security practices throughout the supply chain and to notify NICC.
- The vendor must only use NICC **Information Resources** for the purpose of the business agreement.
- Work outside of defined parameters in the contract must be approved in writing by the appropriate NICC point of contact.
- Vendor performance must be reviewed annually to measure compliance to implemented contracts or SLAs. In the event of non-compliance with contracts or SLAs regular meetings will be conducted until performance requirements are met.
- Vendor's major IT work activities must be entered into or captured in a log and available to NICC IT management upon request. Logs must include, but are not limited to, events such as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.
- Any other NICC information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.
- Vendor personnel must report all security incidents directly to the appropriate NICC IT personnel within the timeframe defined in the contract.
- NICC IT will provide a technical point of contact for the vendor. The point of contact will work with the vendor to make certain the vendor is in compliance with these policies.
- New vendors must provide NICC a list of key personnel working on the contract.
- Vendors with logical access to information resources must provide non-repudiation authentication mechanisms.
- Vendors must provide NICC with notification of key staff changes within 24 hours of change.
- Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to NICC or destroyed within 24 hours.
- Upon termination of contract, vendors must be reminded of confidentiality and non-disclosure requirements.
- Upon termination of contract or at the request of NICC, the vendor must surrender all NICC badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized NICC IT management.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 7, 13, 15, 16
- NIST CSF: DE.CM
- Vendor Non-Disclosure Agreement/Business Associate 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
		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