Encryption Management Policy, version 1.0.0

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

Encryption Management Policy

Purpose

The purpose of the Nebraska Indian Community College (NICC) Encryption Management Policy is to establish the rules for acceptable use of encryption technologies relating to NICC **Information Resources**.

Audience

The NICC Encryption Management Policy applies to individuals responsible for the set up or maintenance of NICC encryption technology.

Policy

- All encryption technologies and techniques used by NICC must be approved by NICC IT Management.
- NICC IT Management is responsible for the distribution and management of all encryption keys, other than those managed by NICC customers.
- All use of encryption technology should be managed in a manner that permits properly designated NICC personnel to promptly access all data, including for purposes of investigation and business continuity.
- Only encryption technologies that are approved, managed, and distributed by NICC IT may be used in connection with NICC **Information Resources**, other than those managed by NICC customers.
- NICC IT Management will create and publish the NICC Encryption Standards, which must include, at a minimum:
    - The type, strength, and quality of the encryption algorithm required for various levels of protection.
    - Key lifecycle management, including generation, storing, archiving, retrieving, distributing, retiring, and destroying keys.
- All NICC information classified as **confidential** must be encrypted when:
    - Transferred electronically over public networks.
    - Stored on mobile storage devices.
    - Stored on laptops or other mobile computing devices.
    - At rest.
- The use of proprietary encryption algorithms is not permitted, unless approved by NICC IT Management
- The use of encryption for any data transferred outside of the United States must be formally approved by NICC IT Management prior to transfer.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 10, 14, 18
- NIST CSF: PR.DS
- Information Classification and Management 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			Document Origination
		4-23-2024	Administrative Council	Review and Approved
		5-7-2024	IT Committee	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