Change Control Policy, version 1.0.0

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

Change Control Policy

Purpose

The purpose of the Nebraska Indian Community College (NICC) Change Control Policy is to establish the rules for the creation, evaluation, implementation, and tracking of changes made to NICC **Information Resources**.

Audience

The NICC Change Control Policy applies to any individual, entity, or process that create, evaluate, and/or implement changes to NICC **Information Resource**.

Policy

- Changes to production NICC **Information Resources** must be documented and classified according to their:
    - Importance,
    - Urgency,
    - Impact, and
    - Complexity.
- Change documentation must include, at a minimum:
    - Date of submission and date of change,
    - Owner and custodian contact information,
    - Nature of the change,
    - Change requestor,
    - Change classification(s),
    - Roll-back plan,
    - Change approver,
    - Change implementer, and
    - An indication of success or failure.

- Notification to impacted users of change timeframe.
- Changes with a significant potential impact to NICC **Information Resources** must be scheduled.
- NICC **Information Resource owners** must be notified of changes that affect the systems they are responsible for.
- Authorized change windows must be established for changes with a high potential impact.
- Changes with a significant potential impact and/or significant complexity must have usability, security, and impact testing and back out plans included in the change documentation.
- Change control documentation must be maintained in accordance with the NICC Data Retention Schedule.
- Changes made to NICC customer environments and/or applications must be communicated to customers, in accordance with governing agreements and/or contracts.
- All changes must be approved by the Information Resource Owner or Chief Information Officer.

- Emergency changes (i.e. break/fix, incident response, etc.) may be implemented immediately and complete the change control process retroactively.

Software Development

- Code development that transmits, uses, or has access to confidential or internal, which includes student information is not allowed without preapproval.
- All approved code must be designed and developed based on the OWASP principles.
- Approved code development must always use test data and never use confidential, internal, or other protected information.
- Approved code development must follow a defined software development life cycle that includes:
  - Training phase
  - Requirements phase
  - Design phase
  - Build phase
  - Test and verification phase
  - Release phase
- All approved code development must be developed and tested in a test environment.
- All approved code development must have a documented security impact evaluation.
- All approved code development must have automatic DAST and SAST reviews and flaws have documented remediation plans.
- All approved code development must have defined dates for periodic reviews.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 12.1.2
- NIST CSF: PR.IP-3
- Network Management Policy
- Data Retention Schedule

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	April 2024			Document Origination
		4-23-2024	Administrative Council	Review and Approved
		5-7-2024	IT Committee	Add notification to affected users. 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