Continuity and Recovery Policy, version 1.0.0

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

Continuity and Recovery Policy

Purpose

The purpose of the Nebraska Indian Community College NICC Continuity and Recovery Policy is to provide direction and general rules for the creation, implementation, and management of the NICC Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).

Audience

The NICC Continuity and Recovery Policy applies to individuals accountable for ensuring business continuity and disaster recovery processes are developed, supported, tested, and maintained.

Policy

Business Continuity

Business Continuity focuses on sustaining the organization's critical business processes during and after a disruption.

- NICC must create and implement a Business Continuity Plan ("BCP").
- The BCP must be periodically tested, and the results should be shared with executive management.
- The BCP must be reviewed and updated upon any relevant change to the organization, at the conclusion of plan testing, or least annually.
- The BCP must be communicated and distributed to all relevant internal personnel and executive management.
- Business continuity planning should ensure that:
    - the safety and security of personnel is the first priority;
    - an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience, and competence;
    - documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event.
- The BCP must include, at a minimum:
    - A risk assessment for critical business processes and operations (Business Impact Analysis);
    - An inventory of critical systems and records, and their dependencies;
    - Requirements for ensuring information security throughout the process;
    - Identification of supply chain relationships and the organization's role to support critical infrastructure;
    - Processes to ensure the safety of personnel;
    - Communication strategies for communications both inside and outside the organization;
    - Mitigation strategies and safeguards to reduce impact;
    - Strategies to address and limit the reputational impact from an event;

- Contingency plans for different types of disruption events;
- Protection and availability of plan documentation;
- Procedures for plan tests, review, and updates.

Disaster Recovery

Disaster Recovery focuses on restoring the technology systems that support both critical and day-to-day business operations.

- NICC must create and implement a Disaster Recovery Plan ("DRP") to support business objectives outlined in the (BCP/critical processes identified by a Business Impact Analysis).
- The DRP must be tested annually, at a minimum.
- The DRP must be reviewed and updated upon any relevant change to IT Infrastructure, at the conclusion of plan testing, or least annually.
- The DRP must be communicated and distributed to all relevant internal personnel and executive management.
- The NICC DRP must include at a minimum:
  - Roles and responsibilities for implementing the disaster recovery plan;
  - List of potential risks to critical systems and sensitive information;
  - Procedures for reporting disaster events, event escalation, recovery of critical operations, and resumption of normal operations;
  - Requirements for ensuring information security throughout the process;
  - An inventory of backups and offsite storage locations;
  - Contingency plans for different types of disruption events;
  - Protection and availability of plan documentation;
  - Procedures for plan tests, review, and updates.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 17
- NIST CSF: ID.BE, PR.IP, RS.RP, RS.CO, RS.IM, RS.RP, RC.IM, RC.CO
- Information Classification and Management Policy
- Business Continuity Plan
- Disaster Recovery Plan

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
		5-30-2024	**IT committee**	
		10-25-2024	**Academic Committee**	**Review and approved**
		12-18-2024	**Administrative**	**Review and approved**
		01-22-2025	**Executive**	**Review and approved**
		03-29-2025	**Board of Directors**	**Review and approved**