UNIVERSITY OF Nebraska

LINCOLN | OMAHA | KEARNEY | MEDICAL CENTER

Effective: *08/08/2022*
Last Revised: *08/08/2022*

Responsible University Administrator:
Assistant Vice President, IT Security Services

Responsible University Office:
Information Technology Services

Policy Contact:
IT Security Services
security@nebraska.edu

ITS-12: Recovery Standard

Standard Contents

1. Purpose

The purpose of the System Recovery Standard is to define the organization's requirements for enforcing effective system recovery practices. This policy defines the requirements pertaining to the creation, testing, and reviewal of recovery mechanisms in place.

2. Scope

This standard shall apply to all The University of Nebraska ("The University") technology assets. Any information not specifically identified as the property of other parties, that is transmitted or stored on Information Systems (including email, messages, and files) shall be considered the property of The University and to which this standard applies. All users (employees, contractors, vendors, or others) of Information Systems are responsible for adhering to this standard.

3. Standard Statement

It is the intention of this policy to establish recovery testing procedures pertaining to data owned by The University. Deviations from the requirements defined herein in the form of exceptions must be approved in advance and in writing by the Chief Information Security Officer ("CISO") as defined in **ITS Policy Exception Standard**. The following subsections outline the System Recovery Standard.

4. System Recovery Requirements

4.1 Backup Recovery Requirements

4.1.1 Business Impact Analysis

Business systems must undergo periodic business impact analysis to identify and document the system's criticality to business operation and to document business backup frequency and recovery requirements.

4.1.2 System Recovery Plans

Recovery procedures must be established for business systems rated as medium or high risk in the Asset Management System. The steps needed to recover data and systems in the event of a business disruption or loss event must be documented. Documented procedures must be periodically reviewed and updated by system owners and administrators.

4.1.3 Regularly Perform Data Backup

Comprehensive automatic backups must be completed to ensure business effectiveness and continuity for systems that have been deemed as necessary by the business. Backups must be completed on a regular schedule as agreed. Data backups must be monitored to ensure that backups are completed as scheduled.

4.1.4 Backup Resiliency

Backups must be processed and stored in a manner that is resilient to physical disasters or malicious cyber-security attacks, such as storing off-site backups. At least one offline and offsite backup of critical data must be maintained to ensure data recoverability. Critical systems will be backed up as a complete system through imaging, or virtual machine copies when running in University virtual environment.

4.1.5 Data Backup Testing

Recovery exercises must be performed on a periodic basis for essential business systems to ensure that backup data is intact and that technology support teams can adequately recover systems in the event of a business disruption in alignment with business requirements. Where exceptions are noted, system owners must review and update recovery procedures to address identified issues.

4.1.6 Protect the Confidentiality of Backup CUI
Backup data must be secured in a manner consistent with the protections of its corresponding production data, in accordance with the **System and Informational Integrity Standard** and the **Media Protection Standard**. This protection must include:

- Encryption of CUI backup data
- User access restriction based on the principle of least privilege
- Physical security of media and areas containing CUI backup data

4.1.7 Third Party Backup Services
Third parties utilized in the performance, transport, or storage of University backup data must be formally authorized and vetted for appropriate security mechanisms and controls in alignment with established vendor risk management processes prior to use.

5. Procedures

Procedures specific to this Standard are to be documented and maintained by the individual service owners throughout the University system.

6. Compliance

Compliance Measurement
The University of Nebraska IT Security Services team will verify compliance to this Standard through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Standard owner.

Exceptions
Any exception to the Standard must be documented and formally approved by the CISO. Standard exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the Standard exception is required
- Any risks created by the Standard exception
- Risk mitigation plan and duration of the exception
- Evidence of approval following established Exception Standard

Non-Compliance
Failure to comply with University IT standards may result in sanctions relating to the individual's use of IT resources or other appropriate sanctions according to policies applicable to University faculty and staff or student conduct.

7. Related Information

The following is a listing of related Policies, Executive Memoranda, Standards, Controls, and Procedures.

NIST 800-53
NIST 800-171
NU Executive Memorandum 16
NU Executive Memorandum 26
NU Executive Memorandum 41
NU Executive Memorandum 42

University-Wide Policies & Guidelines - https://nebraska.edu/offices-policies/policies
ITS-00 Information Technology Definitions and Roles
ITS Knowledge Base - https://uofnebraska.sharepoint.com/sites/NU-ITS/KB

8. Approvals and Revision History

Approval of this Standard:

	Name	Title	Date
Authored by:	Richard Haugerud	IT CISO	08/08/2022
Approved by:	Bret Blackman	IT CIO	08/08/2022

Revision history of this Standard:

Version	Date	Description
1.0	08/08/2022	Initial Standard Published