UNIVERSITY OF Nebraska® System

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-08: Systems Maintenance Standard

Standard Contents

1. Purpose 2
2. Scope 2
3. Standard Statement 2
4. Systems Maintenance Requirements 2
   4.1 Maintenance Management 2
5. Procedures 3
6. Compliance 3
7. Related Information 3
8. Approvals and Revision History 4

1. Purpose

The purpose of the System Maintenance Standard is to define the organization’s requirements for enforcing effective system maintenance procedures. Proper maintenance and support of University assets increases usability and lowers the total cost of ownership to the organization, while also strengthening system security posture. This Standard is designed to support preventative and ongoing maintenance of University hardware and software assets to achieve these objectives.

2. Scope

This Standard shall apply to all University of Nebraska System (“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 Standard to establish a systems maintenance capability throughout the University to help the organization implement security best practices regarding the development and maintenance of University information systems. 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 Maintenance Standard.

4. Systems Maintenance Requirements

4.1 Maintenance Management

4.1.1 Controlled Maintenance

University service, data owners / stewards and IT support teams must schedule and perform regular maintenance on IT assets (including hardware, firmware, software, and applications), in accordance with vendor specifications, to ensure effective functionality over the asset’s planned lifecycle. Funding should be allocated annually to account for ongoing maintenance, functionality updates, and security updates.

All maintenance activities must be controlled, scheduled, and approved prior to implementation in production in accordance with the Change Control Procedures and **Configuration Management Standard**. Maintenance activities must be documented to indicate, at a minimum:

- The date and time of the performed maintenance
- Name of individual(s) performing maintenance activities
- A description of maintenance activities performed
- Information system components and equipment in-scope for performed maintenance, including any system components or equipment removed or replaced.

4.1.2 Authorized Maintenance Personnel

All maintenance activity must be performed only by authorized personnel. The University must establish processes for authorizing qualified maintenance organizations and personnel and ensuring that they are appropriately trained to ensure system maintenance is upheld. Any maintenance activities performed by individuals or organizations that were not previously authorized, such as in the event of emergency maintenance, must be escorted and/or supervised by authorized maintenance staff.

4.1.3 Remote Maintenance

All maintenance activities performed over network connection, including remote maintenance performed by third parties, must be secured via strong encryption, multi-factor authentication, and appropriate least privilege, in accordance with the **Access Control Standard**. All maintenance sessions must be monitored and must be allowed to remain active only for the duration necessary to perform maintenance activities.

4.1.4 Maintenance Tools

Tools used in maintenance activities for diagnostic and repair activities on University information systems, including hardware, software, and firmware, must be authorized prior to use. Prior to implementation of the maintenance tool, procedures must be exhibited to scan any installation files for any corruption or malicious code.

4.1.5 Maintenance Security Control Validation

Following maintenance completion, IT support teams must test and validate all potentially impacted security controls to verify that the controls are working as intended.

4.1.6 Off-Site Maintenance

IT Support Management and data stewards / owners must explicitly approve the removal of all information assets or system components from organizational facilities for off-site maintenance or repairs prior to transfer. All equipment taken offsite must first be sanitized to remove all stored data, using approved methods, in accordance with the **Media and Protection Standard**.

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