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

Asset Management Standard

Standard Contents

1. Purpose

The Asset Management Standard defines the organization's requirements governing the management of information technology assets. These assets include physical, virtual, software, and non-public institutional and research data assets (refer to **Executive Memorandum 42**) from receipt and inception to final disposal. It includes requirements for the maintaining of an accurate, up-to-date inventory, as well as requirements for the classification of assets based up on their value to The University of Nebraska System ("University") and its affiliates.

2. Scope

This Standard shall apply to all 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 an Asset Management capability throughout the University of Nebraska to help implement security best practices regarding inventory and management of information and IT assets. 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 Asset Management Standard.

4. Asset Management Requirements

4.1 Asset Management

4.1.1 Asset Inventory

IT hardware and software assets, including loaned or demo equipment, must be identified, recorded, maintained, and tracked in centralized asset management reporting throughout the asset's lifecycle. In the absence of a centralized asset management platform, University organizations will be responsible for maintaining an inventory of IT hardware and software assets. Asset management systems must be authorized, assigned an owner, and enforce appropriate role-based access in alignment with the University **Access, Identification and Authorization Standard.** IT asset records must include minimum attributes as defined within this Standard. Each asset or group of assets must have a risk classification (Low, Med, High) assigned per **Executive Memorandum 42**, the **Risk Management Standard** or via a FIPS 199 exercise. Deviations or exceptions from these minimum attributes must be authorized by management and logged within the asset management system.

4.1.2 Hardware Asset Records Minimum Attributes

Hardware asset records must include, at a minimum, the following attributes:

- Asset name or unique identifier (e.g. asset tag, hardware name, network name)
- Risk classification based on type(s) of data stored, processed or transmitted
- Network information (MAC address and IP address(es), if static)
- Unique identifier (e.g. serial number); refer to **Endpoint Baseline Procedure**
- Asset type (desktop, laptop, server, virtual machine, mobile, network device, IoT device, etc.)
- Physical Location
- Cost center or assigned business unit
- Asset Owner (Business owner)
- Manufacturer
- Asset status (deployed, decommissioned, storage, maintenance, etc.)
- Acquisition category (purchased, leased, rental)
- Asset acquisition date
- Asset life expectancy

4.1.3 Information System & Software Asset Record Minimum Attributes

Software asset records must include, at a minimum, the following attributes:

- Asset name
- Risk classification based on type(s) of data stored, processed or transmitted
- System / Asset owner
- System / Asset administrator (who is maintaining this application)
- Patch Date
- System / Asset version
- System / Asset purpose
- Hardware asset software is located on (if applicable)
- Manufacturer
- Asset status
- Number of asset licenses owned
- Number of assets deployed
- IT license type (e.g. user based, enterprise etc.)

4.1.4 Asset Inventory Reconciliation

IT Asset Owners must periodically reconcile assets within the asset management system to ensure completeness and accuracy of asset records and related attributes. Any changes to asset record attributes resulting from reconciliation or ongoing business processes must be authorized by the asset owner and logged within the asset management system.

4.1.5 Unauthorized Assets

Any unauthorized IT hardware and software assets identified on the University network through IT asset reconciliation processes must be reported to ITS Security Services for appropriate incident response, in alignment with the **Incident Response Standard**.

4.1.6 Inactive Hardware Assets

Identified inactive hardware assets must be properly updated and managed, including the timely and secure return of assets to appropriate storage facility in alignment with established procedures. Inactive hardware is hardware that is no longer being actively used to support University processes and is not planned to be used to support processes in the future.

4.1.7 Hardware Sanitization

IT hardware assets must be sanitized per the **Media and Protection Standard** of any information prior to disposal and disposed of using secure shipment methods in alignment with established IT hardware disposal procedures. Disposal requests must be documented and must be performed by approved vendors. Certificates of disposal must be obtained for all IT hardware asset disposals. Following disposal, Asset Owners must update asset records to reflect disposal status. The asset record must remain in the asset management system in a “disposed or decommissioned” status until the data retention limit has been reached.

4.1.8 Hardware Re-Use

Prior to asset re-use within the organization, IT hardware must be sanitized per the **Media and Protection Standard**, re-formatted, and re-imaged using an approved system image and configuration baseline, in accordance with the **Configuration Management Standard** and hardware sanitization procedures. Any changes to the asset owner and administrator must be updated.

4.1.9 Maintenance

Asset owners and asset administrators are responsible for performing proper maintenance of IT Assets under their control. This will ensure the asset is functioning effectively and securely over its planned lifecycle, in accordance with the **Systems Maintenance Standard**.

4.1.10 Software License Management

All software acquisitions and license purchases over a pre-determined amount, defined by University of Nebraska Procurement, must be authorized by University Procurement to ensure alignment with enterprise contractual agreements. During required periodic software inventory reconciliation activities detailed in this Standard, identified inactive licenses should be reclaimed by asset owners. These licenses should be redeployed prior to any purchase of new licenses.

Once a software asset has reached the end of its useful life, the asset owner must update the status of the asset record and remove the software from the inventory of enterprise software available for request. The asset owner must also ensure that all licenses have been deactivated and the retired software is no longer in use across the organization.

4.2 Asset Protection and Handling

4.2.1 Acceptable Use of Assets

The acceptable use of assets is governed through **Executive Memorandum 16**. The University must ensure that all users of assets are made aware of the information security requirements as well as their responsibility to return the asset upon termination.

4.2.2 Physical Security of Assets

All assets must be stored in physically and environmentally secure environments in accordance with the **Physical Protection Standard** and manufacturer specifications.

4.2.3 Data Handling

Information assets containing University data must be classified, protected, and handled in a manner corresponding to their risk classification, in accordance with **Executive Memorandum 42** and **Media and Protection Standard**.

5. Standards and 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