University System of New Hampshire

Inventory Management of Information Technology Assets Standard

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: Cybersecurity & Networking
Approved Distribution: PUBLIC
Status: In-Force

1. Purpose

The purpose of this standard is to establish a set of guidelines and procedures for the management, tracking, and maintenance of information technology (IT) inventory within the university. Effective IT inventory management is essential to ensure efficient use of resources, security, compliance, and continuity of IT services.

2. Scope

This standard applies to all USNH USNH staff, faculty, students, affiliates, contractors, and third-party service providers who handle university data and information systems.

3. Standard

3.1 Asset Identification and Labeling:

Each IT asset must be cataloged and when possible, assigned a unique identification number or barcode.

Assets should be labeled clearly with this identifier for easy tracking and management.

3.2 Documentation:

Maintain an accurate and up-to-date inventory database or management system.

Include essential information for each asset, such as asset type, manufacturer, model, serial number, purchase date, warranty status, location, and assigned user.

3.3 Procurement and Acquisition:

All IT purchases must adhere to the university's procurement policies and procedures.

Document all purchase transactions and ensure proper approvals are obtained.

3.4 Asset Tracking:

Conduct regular physical and digital audits to verify the existence and status of IT assets.

Update the inventory database promptly to reflect changes, such as new acquisitions, movements, disposals, or upgrades.

3.5 Asset Lifecycle Management:

Implement a lifecycle management strategy for IT assets, including maintenance schedules, upgrades, and end-of-life procedures.

Dispose of outdated or non-functional assets in compliance with university and environmental regulations.

3.6 Security Measures:

Protect IT assets from theft, damage, or unauthorized access.

Implement access controls, surveillance, and physical security measures, as necessary.

3.7 Software and Licensing:

Maintain an inventory of software licenses and ensure compliance with licensing agreements.

Regularly audit software installations to verify license usage.

3.8 Backup and Recovery:

Implement backup and disaster recovery plans for critical IT assets and data.

Test and update these plans regularly to ensure they remain effective.

3.9 Reporting:

Generate and distribute regular reports on IT inventory status, including asset utilization, maintenance, and compliance with relevant policies and standards.

3.10 Training and Awareness:

Provide training and awareness programs for personnel involved in IT inventory management.

Ensure they understand their responsibilities and follow best practices.

3.11 Disposal and Recycling:

Dispose of outdated or obsolete IT assets in an environmentally responsible manner.

Ensure data destruction is carried out securely, following established procedures.

3.12 Compliance and Auditing:

Conduct periodic audits to verify compliance with this standard.

Address any identified non-compliance issues promptly.

4. Exceptions

Requests for exceptions to this Standard shall be submitted and approved according to the requirements provided in the Cybersecurity Exception Standard.

5. Enforcement

Anyone found to have violated this policy may be subject to disciplinary action, up to and including suspension of access to institutional resources or termination of employment. Students may be referred to Student Affairs for discipline. A violation of this policy by a temporary worker, contractor or vendor may result in action up to and including termination of their contract or assignment with USNH.

Employees who are members of institutionally recognized bargaining units are covered by the disciplinary provisions set forth in the agreement for their bargaining units.

Contact Information

For a comprehensive list of all Policies and Standards, visit the USNH Cybersecurity Policies & Standards page.

For USNH community members: Questions about this Standard, requests for additional information or training, or reports of violations can be directed to Cybersecurity Governance, Risk, and Compliance (GRC) via this Support Form.

All other requests can be submitted here: Submit an IT Question.

DOCUMENT HISTORY

Effective Date:	February 2, 2024
Approved by:	Thomas Nudd, CISO
Reviewed by:	Dr David A Yasenchock, Director, Cybersecurity GRC
Revision History:	V 1.0

University System of New Hampshire