University System of New Hampshire

SECURE CONFIGURATION MANAGEMENT STANDARD

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

1 PURPOSE

This Standard aims to establish procedures and policies for configuration management of the University System of New Hampshire's (USNH) information technology resources.

2 SCOPE

This standard applies to all USNH business and academic units and USNH-owned information systems that collect, store, process, share or transmit institutional data. Personally owned devices that connect to the University Campus Network must meet the requirements of the Bring Your Own Device Standard.

3 AUDIENCE

All USNH community members who access USNH information technology resources should be familiar with this Standard

4 STANDARD

4.1 INFORMATION SYSTEM COMPONENT INVENTORY

Secure configuration management requires an accurate, up-to-date inventory of information technology resources. ET&S teams configuring, installing, or deploying new USNH information technology resources shall develop and document an inventory of information system components that:

- Reflects the current information system accurately.
- Includes all components within the authorization boundary of the information system.
- Is at the level of granularity deemed necessary for tracking and reporting.
- Includes information considered necessary to achieve effective information system component accountability.
- Review and update the information system component inventory annually.
- Update the inventory of information system components as an integral part of component installations, removals, and information system updates.

University System of New Hampshire

4.2 CONFIGURATION MANAGEMENT PLAN

IT shall develop, document, and implement a configuration management plan for the information system that:

- Addresses roles, responsibilities, and configuration management processes and procedures.
- Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.
- Defines the configuration items for the information system and places the configuration items under configuration management.
- Protects the configuration management plan from unauthorized disclosure and modification.

4.3 BASELINE CONFIGURATION

A baseline configuration is the settings originally applied to the system to ensure it operates as intended. ET&S teams configuring, installing, or deploying new USNH information technology resources shall:

- Maintain secure configuration baselines for servers and endpoints throughout the system development life cycle (SDLC). Baseline configurations shall conform to industry best practices and may be created from pre-built configuration templates. Baseline configurations shall be updated periodically (with corresponding updates to change management logs and other pertinent documentation) as the system configurations change based on operational requirements and new security threats.
- The current and previous versions of configuration baselines must be stored in a secure location. One earlier version, at a minimum, of a configuration baseline, must be retained to support rollback and recovery. Validation and confirmation of configuration settings are strongly encouraged and may be done using automated tools.
- In all instances, the configuration baseline must be documented, reviewed, and updated at least annually and upon significant changes to information system functions, roles, or architecture.

4.4 CONFIGURATION CHANGE CONTROL

ET&S teams configuring, installing, or deploying new USNH information technology resources shall:

- Determine and document the types of physical and logical changes that are configuration-controlled.
- Analyze changes to the information system to determine potential security impacts before change implementation.

- Coordinate and provide oversight for configuration change control activities through The Change Advisory Board (CAB), which convenes weekly or as needed. Approved controlled changes shall be documented and logged.
- Implement approved configuration-controlled changes to the information system.
- Retain records of configuration-controlled information system changes for at least two years.
- Audit and review activities associated with configuration-controlled changes to the information system.

The Change Advisory Board shall review proposed configuration-controlled changes and approve or deny such changes with explicit consideration for security impact. The CAB shall document controlled configuration change decisions and retain records for at least two years.

4.5 LEAST FUNCTIONALITY

ET&S teams configuring, installing, or deploying new USNH information technology resources shall:

- Configure the information system to provide only essential capabilities.
- Review the information system quarterly to identify unnecessary and/or non-secure functions, ports, protocols, and services.
- Disable functions, ports, protocols, and services within the information system deemed unnecessary and/or non-secure.
- Prevent program execution in accordance with policies regarding software program usage and restrictions and rules authorizing the terms and conditions of software program usage.
- Identify software programs not authorized to execute on information systems.
- Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system.
- Review and update the list of unauthorized software programs annually.

4.6 SOFTWARE USAGE RESTRICTION

ET&S shall:

- Use software and associated documentation in accordance with contract agreements and copyright laws.
- Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.

5 MAINTENANCE OF PROCESSES AND PROCEDURES RELATED TO THIS STANDARD

University System of New Hampshire

As part of the mandatory annual review of this Standard required by the *USNH Cybersecurity Policy*, the processes and procedures that support the requirements defined in this Standard shall be reviewed and, where needed, updated to ensure currency and continuous improvement.

6 ENFORCEMENT

Failure to comply with this Policy puts the University System, its component institutions, and its information and information technology resources at risk and may result in disciplinary action. Disciplinary procedures will be appropriate for the individual responsible for non-compliance (e.g., students, faculty, staff, vendors) as outlined in the relevant institutional regulations for that individual (e.g., student conduct and/or applicable personnel policies).

Non-compliant technology and/or activities may be mitigated as deemed necessary by the CISO and/or CIO.

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

7 EXCEPTIONS

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

8 DEFINITIONS

- Baseline Configuration
- System Development Life Cycle (SDLC)
- Change Control
- Change Advisory Board (CAB)
- Least Functionality
- Allow-All, Deny-By-Exception

9 RELATED POLICIES AND STANDARDS

University System of New Hampshire Cybersecurity Policy

University System of New Hampshire Acceptable Use Policy

Endpoint Management Standard

Network Security Standard

University System of New Hampshire

CONTACT INFORMATION

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:	December 16, 2022
Approved by:	Dr David A Yasenchock, Interim CISO
Reviewed by:	Dr David A Yasenchock, Director, Cybersecurity GRC
Revision History:	V 1.00