University System of New Hampshire

Endpoint 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 defines the minimum required security controls for endpoint devices (e.g., desktop computers, laptops, tablets, or similar) owned by the University System of New Hampshire (USNH) or one of its component institutions used to conduct USNH business or connected to a USNH network. These controls help to safeguard the confidentiality, integrity, and availability of USNH information and information technology resources by reducing the risk of Cybersecurity incidents resulting from:

- The connection of improperly secured endpoint devices to USNH networks
- The use of improperly secured endpoint devices in conjunction with non-public institutional information
- The compromise and/or destruction of institutionally owned endpoints, information, and /or information technology resources

2. Scope

This Standard applies to:

All institutionally owned endpoint devices.

Personally owned endpoint devices used to conduct USNH business.

Personally owned endpoints that are connected to a USNH network or a USNH information technology resource, regardless of how they are used.

Endpoint devices owned by students that, when connected to a USNH network, are only used for academic or personal activities are exempt from all provisions in this Standard except those outlined in the **USNH Network Access for All Endpoints** section below.

IT affiliates (e.g., CCOM. SWRI) co-located on a component institution campus shall adhere to endpoint device management requirements for any endpoint device connecting to a USNH network.

For purposes of this Standard, mobile phones, game consoles, and Internet of Things (IoT) devices are not considered endpoint devices. Specific requirements for these types of devices are defined in another standard.

3. Standard

3.1 Institutionally Owned Endpoints

All institutionally owned endpoints shall be physically protected to prevent access by unauthorized persons, shall not be shared with or used by unauthorized persons, and shall, at a minimum, have the following protections implemented.

3.1.1 Configuration

The information below provides basic requirements for securely configuring endpoint devices. Specific details about how security configuration baselines for endpoints are established, reviewed, and modified are provided in the *Security Configuration Management Standard*.

Additionally, each institutional endpoint shall be configured such that:
It is running a current, non-deprecated version of an operating system that can be updated whenever new security patches are available.
The endpoint's firewall is activated and configured.
All institutional endpoints display the USNH login
banner.
It automatically locks after 15 minutes of inactivity for Workstations (i.e., desktops, laptops, etc.) and 2 minutes of inactivity for remote devices (i.e., iPads, Tablets, etc.).
Access to the device is secured using the appropriate institution’s central authentication, where the use of central authentication is technically possible.
If this is not possible, an exception must be requested and granted before access to an endpoint can be configured using alternate credentials.
Management

Institutionally owned endpoint devices shall be centrally managed using automated endpoint configuration management tools provided and managed by Enterprise Technology & Services (ET&S).
At a minimum, central management shall include:

Installation and automated updates of a configuration management client, where
appropriate.
Delivery of operating system, firmware, and application-specific security patches.
Deployment of institutionally approved anti-malware software.
Monitoring to ensure anti-malware software is providing active protection, that scans are being performed regularly, and that the definitions used by the tool are being updated regularly.
Notify security issues found on the device to appropriate security or desktop management personnel.
Monitoring of adherence to these and other required controls outlined in this Standard.

3.1.2 Support and Maintenance

ET&S shall be responsible for the support and maintenance of all institutional devices.

3.1.3 Patching/Updating

Security updates/patches shall be applied within four weeks of release. If a security update/patch must be deployed in a shorter timeframe to protect USNH information technology resources, the Chief Information Security Officer shall be empowered to impose an expedited timeframe on all institutionally owned devices. In these circumstances, best effort shall be made to provide adequate communication of the expedited timeframe to those community members responsible for security patch deployment on their institutionally owned devices.

Failure to update an endpoint device according to this timeline may result in the endpoint being blocked from accessing any USNH network or information technology resources until the device is compliant.

ET&S shall be responsible for testing the operating system, firmware updates, and software patches for effectiveness and potential side effects before deploying via automated endpoint configuration management tools.

3.1.4 Monthly Restart

All institutionally owned endpoint devices shall be restarted at least once a month to ensure all available security patches have been installed. Failure to restart an endpoint within this timeframe may result in the endpoint being forcibly restarted by ET&S.

3.1.5 Software

Any software installed on endpoints shall be appropriately licensed and used in a manner that complies with all USNH and institution-specific policies and any licensing requirements.

3.1.6 Endpoint Encryption

All institutionally owned endpoint devices shall be encrypted with full-disk encryption using the institutionally supported and managed endpoint encryption solution.

Institutionally owned endpoint devices provided in kiosks, public computer labs, and classrooms that process Public Information are not required to be encrypted.

3.1.7 Purchase of Institutionally Owned Endpoints

Administrative, academic, and business units shall purchase all institutional endpoints through the approved endpoint purchasing program administered by ET&S.

3.1.8 Repair of Institutionally Owned Endpoints

Endpoints needing repair shall be repaired through the approved institutional vendor(s) and cannot be taken to unapproved third-party providers for service or repair.

Prior to being sent off-campus for repair, endpoints shall be encrypted with full-disk encryption using the institutionally supported and managed endpoint encryption management solution. Suppose an endpoint in need of repair cannot be encrypted. In that case, the endpoint's hard drive shall be removed by the institution's approved provider and stored securely, using a mechanism approved by the Chief Information Security Officer (CISO), until the endpoint is returned to the institution.

3.1.9 Local Administrator Accounts

A Local Administrator Account, defined as a local account with full administrative privileges to the endpoint, on institutionally owned endpoints shall be limited to the ET&S Desktop Management team, wherever possible.

Allowing an end-user domain account administrative access to an institutional endpoint is highly discouraged.

Passwords associated with this type of account must be unique and are not considered system administrator accounts for purposes of the USNH Password Policy.

3.1.10 Backup of Endpoint Devices

Institutionally owned endpoint devices are not, by policy or common practice, backed up. Institutional information and documentation should be stored in approved shared file storage to ensure business-critical information and documentation remains available.

3.1.11 System Quarantine

Quarantining systems are essential actions undertaken by Cyber Operations (CYOPs). Once a system is quarantined, CYOPs initiates a Team Dynamix Ticket to Desktop Support and the Help Desk, along with necessary communications to the system owner and their supervisor. Please note that only CYOPs have the authority to quarantine a system.

Reasons for system quarantine include:

- **Indications of Compromise:** Any signs that suggest the system has been compromised.

- **Unprocessed Personal Property:** Systems designated as personal property without undergoing proper processing through desktop support. USNH software on systems is USNH's property and must be removed before disposal, whether as a gift or part of the Seed process.

- **Unresolved Critical Vulnerabilities:** Systems with critical vulnerabilities that haven't been addressed, potentially posing risks to the USNH enterprise.

- **Questionable Activity or Network Traffic:** Systems observed engaging in suspicious activity or network behaviors.

- **Directives from USNH Leadership or Campus Security:** Quarantine directives issued by USNH leadership or Campus Security.

These protocols ensure the integrity and security of systems within the USNH infrastructure, mitigating risks and safeguarding against potential threats.

3.1.12 Traveling Internationally with an Institutionally Owned Endpoint

USNH community members who need to travel internationally with an institutionally owned endpoint shall take appropriate precautions to protect that device and all institutional information stored on it or accessible using it. For assistance in determining the appropriate precautions, contact Cybersecurity & Networking.

3.2 Disposal of Institutionally Owned Endpoints

At end-of-life, institutionally owned endpoints shall be disposed of via the Secure Electronic.

Equipment Disposal (SEED) process. With limited and particular exceptions, institutional endpoints cannot be sold to USNH community members. Contact ET&S – Desktop Management for information on these exceptions.

As part of the disposal process, endpoints shall be removed from Active Directory and relevant central endpoint management tools.

3.3 Personally Owned Endpoints

Personally owned endpoints cannot be used to capture, store (even temporarily), or transmit information classified as RESTRICTED or CONFIDENTIAL.

Remote access to USNH information technology resources by any endpoint device is defined in the *Remote Access and VPN Standard.*

All personal endpoints used to connect to a USNH network and/or that are used to access, capture, process, or otherwise manage institutional information shall have the following protections implemented:

- Access to the endpoint shall be protected by authentication.
- Anti-malware software shall be installed on the endpoint and configured to provide active protection and/or to perform scans on a regular basis.
- An operating system supported by the manufacturer with all available security patches applied shall be installed on the endpoint.
- Personally owned devices shall not get direct access to critical resources, such as joining an internal network domain.

Personal endpoints used to access a USNH network that do not meet these requirements may be blocked from accessing all USNH networks or USNH information technology resources until brought into compliance.

3.4 USNH Network Access for All Endpoints

Endpoints seeking to connect to a USNH network shall be registered with the network's Administrator. This registration process shall associate the unique identifier for the endpoint with the USNH community members' USNH username.

Unregistered endpoints or those whose registration information has become invalid shall not be allowed to connect to a USNH network.

Access to USNH networks by those not affiliated with the University System or any of its component institutions, referred to here as Guest Access, shall be allowed on a limited basis. Guest access shall

also require registration of the endpoint, resulting in the assignment of a temporary

username comprised of the endpoint's MAC address and the first and last name of the endpoint's registrant. Registration of an endpoint for guest access shall expire after one month.

Requirements for remote access of USNH networks by endpoints and using the USNH Virtual Private Network (VPN) are defined in the *Remote Access and VPN Standard.*

5. Exceptions

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

6. 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.

7. 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, & Compliance (GRC) via this Support Form.

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

DOCUMENT HISTORY

Effective Date:	01 MAY 2021
Approved by:	CISO, USNH, T.NUDD, 08 JUN 2021 V1 DIRECTOR, DESKTOP MANAGEMENT, J MOURIKAS, 02 FEB 2021 V1 CYBERSECURITY POLICY & STD WORKING GROUP, 14 JAN 2021 V1
Reviewed by:	CISO, USNH, T NUDD, 08 JUN 2021 V1

	DIRECTOR, DESKTOP MANAGEMENT, J MOURIKAS, FEB 2021 CYBERSECURITY POLICY & STANDARD WORKING GROUP, DEC 2020/JAN 2021
Revision History:	DRAFT REVIEW, T NUDD, 08 JUN 2021 REVIEW DRAFT FINALIZED, R BOYCE-WERNER, 08 MAR 2020 Revised Endpoint Encryption for endpoints that process public information, W SAMES, 04 MAR 2022 Revised Personally Owned Endpoints Section, K SWEENEY 07 JULY 2023 Revised Endpoint Configuration Section, D YASENCHOCK 16 NOV 2023 Revised Contact Information section, K SWEENEY 30 NOV 2023 Added Section 3.1.11, T GIBSON 06 JAN 2024