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 AUDIENCE

This Standard is intended for all members of the USNH community who are provided use of or access to institutionally owned endpoint devices or who use personally owned endpoint devices to capture, store, process, transmit, or otherwise manage institutional information or to connect to a USNH network or information technology resource.

4 STANDARD

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.

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 is capable of being updated whenever new security patches are available.
- The endpoint's firewall is activated and configured.
- All institutional endpoints display USNH login banner.
- It automatically locks after 15 minutes of inactivity.
- Access to the device is secured using the appropriate institution's central authentication, where the use of central authentication is technically possible.
    - In circumstances where 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 on a regular basis, and that the definitions used by the tool are being updated regularly.
- Notification of 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.

Support and Maintenance

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

Patching/Updating

Security updates/patches shall be applied within 4 weeks of release. In the event that 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 who are 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 brought into compliance.

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

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.

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.

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 that are provided in kiosks, public computer labs, classrooms or as loaner devices, do not need to be encrypted.

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.

Repair of Institutionally Owned Endpoints

Endpoints in need of 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. If an endpoint in need of repair cannot be encrypted, 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.

Local Administrator Accounts

The use of a Local Administrator Account, which is 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 to have 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.

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.

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.

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 very specific 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 from relevant central endpoint management tools.

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.

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.

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 who are 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 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 for use of the USNH Virtual Private Network (VPN) are defined in the *Remote Access and VPN Standard.*

5 Maintenance of Processes and Procedures Related to this Standard

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 Standard 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 ROLES AND RESPONSIBILITIES

Administrative, Academic, and Business Leadership:

- Enforce the Cybersecurity controls defined in this Standard across all areas under their control
- Report all Cybersecurity events or incidents to Cybersecurity Ops

Chief Information Security Officer (CISO):

- Monitor adherence to this Standard and related processes and procedures
- Act, with appropriate communication to device owners when possible, to ensure network connected information technology resources including institutionally and personally owned endpoints do not pose a threat to the University System, it's component institutions, it's information, or it's information technology resources
- Review and approve exceptions to this Standard

Desktop Management:

- Ensure all institutionally owned endpoints are configured, deployed, and maintained in accordance with the requirement defined in this Standard
- Check all endpoints that come in for repair for enterprise-approved encryption
- Encrypt institutionally owned endpoints, when needed, prior to them being taken off-site for repair

Cybersecurity GRC:

- Process and track all exceptions to this Standard
- Conduct an audit of security controls used to protect institutionally owned endpoints and institutional information protected by regulation, including those outlined in this Standard

Network Administrators:

- Quarantine or block endpoints attempting to connect to a USNH network that do not comply with this Standard

USNH Community Members:

- Comply with all restrictions and requirements outlined in this Standard
- Take appropriate precautions to protect institutionally owned endpoints from loss, theft, or damage
- Understand the classification of all institutional information they capture, store, process, transmit, or otherwise manage to ensure the use of appropriate safeguards
- Report all Cybersecurity events or incidents to Cybersecurity Ops

9 DEFINED TERMS

See the ET&S Policy & Standard Glossary for full definitions of each term.

- Access
- Account
- Anti-Malware Software
- Availability
- Baseline
- Central Authentication
- CONFIDENTIAL Information
- Confidentiality
- Configuration Management
- Credentials
- Encryption
- Endpoint Device
- Exception
- Firewall
- Information
- Cybersecurity Incident
- Information Technology Resource
- Institutional Information
- Institutionally Owned Endpoint
- Integrity
- MAC Address
- Password

University System of New Hampshire

- Patch
- Personally Owned Endpoint
- Policy
- Portable Device
- RESTRICTED Information
- Security Configuration Baseline
- Security Control
- Standard
- Username
- USNH Community Member
- Vendor

10 Related Policies and Standards

- Cybersecurity Policy
- Information Classification Policy
- Password Policy
- Cybersecurity Exception Standard
- Remote Access and VPN Standard
- Security Configuration Management Standard

---

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

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

---

DOCUMENT HISTORY

Effective Date:	10 AUG 2021
Approved by:	CISO, USNH, T.NUDD, 08 JUN 2021 V1 DIRECTOR, DESKTOP MANAGEMENT, J MOURIKAS, 02 FEB 2021 V1

University System of New Hampshire

	CYBERSECURITY POLICY & STANDARD 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