University System of New Hampshire

PRIVATELY MANAGED NETWORK STANDARD

Responsible Executive/University Officer: Chief Information Security Officer
Responsible Office: Cybersecurity & Networking
Authorized Distribution: PUBLIC
Status: IN REVIEW

1 PURPOSE

The University System of New Hampshire (USNH) must provide a secure network for our educational, research, instructional and administrative needs and services. Protection of the University System's networks is critical to ensuring the confidentiality, integrity, and availability of institutional information and to the ongoing support of all component institution operations. The following Standard is designed to inform members of the USNH community who have a business need for a privately managed network space about the security controls required to protect USNH networks from accidental, or intentional damage, and from alteration or theft of information while preserving appropriate access and use by the USNH community.

The purpose of this Standard is to define the minimal acceptable configuration for connecting privately managed networks to any USNH network. An unsecured network creates conditions that increase the risk of denial of service attacks, malware infections (viruses, Trojans, etc.) and other attacks aimed at compromising the integrity of the network and any devices connected to it. Damages from these types of attacks could include the loss of sensitive and restricted data, interruption of network services, and damage to critical internal systems, resulting in loss of reputation/brand damage, loss of productivity, and significant financial cost. Therefore, individuals who connect network hardware to a USNH network must follow specific standards and take specific actions.

The minimum acceptable configuration is designed to:

- Minimize exposure to the University System, its component institutions, and our community from the potential damages (including financial, reputational, loss of work, and loss of data) resulting from servers and network hardware that are not configured or maintained properly
- Ensure that devices on USNH networks are not taking actions that could adversely affect network performance

University System of New Hampshire

2 SCOPE

The mandated procedures and practices outlined here apply to all UNH community members who support network switch and routing technologies.

3 AUDIENCE

This Standard informs all USNH and component institution personnel, students, contractors, and vendors of the expectations around the management of any privately managed networks that connect to any of the USNH networks.

4 STANDARD

As outlined in each institution's Acceptable Use Policy/Computer and Network Use Policy, the use of network equipment and software is prohibited unless specifically authorized by the Network System Administrator.

Enterprise Technology & Services (ET&S), as the Network System Administrator of each institution's network, is responsible for providing reliable network services at each of the USNH Institutions. As such, individuals or departments shall not run any service which disrupts or interferes with centrally provided services.

These services include, but are not limited to:

- Privately managed networks
- DNS (Domain Name System)
- DHCP (Dynamic Host Configuration Protocol)
- Domain Registration

PRIVATELY MANAGED NETWORK REQUIREMENTS

In some circumstances, an exception can be granted per the process outlined below. For an exception to be granted:

- Specific network configuration elements must be deployed within the privately managed network
- Personnel in requesting departments must demonstrate competence with managing the privately managed network to the expected minimum configuration.

Required Privately Managed Network Oversight

All privately managed networks must be overseen by a USNH employee. Students and sponsored users cannot request or oversee a privately managed network.

University System of New Hampshire

Required Network Configuration Elements

ET&S uses multiple methods to protect the USNH institutional networks, including monitoring for external intruders, scanning hosts on the network for suspicious anomalies, and blocking harmful traffic.

To ensure these protections extend to all privately managed networks, the following elements must be deployed and meet the standards set by the Network System Administrator, when operating a privately managed network:

- Boundary Protection via Firewall as outlined in NIST SP 800-53 SC-7
- Vulnerability Scanning as outlined in NIST SP 800-53 RA-5
- Network Access Controls as outlined in NIST SP 800-53 AC-2

All these configuration elements shall have a current vendor support contract in place.

All network equipment shall be configured to log to a central log repository.

All network traffic passing in or out of a USNH network to/from the privately managed network shall be monitored by an intrusion detection system (IDS) for signs of compromises.

Required Network Protection Activities

Personnel approved to operate privately managed networks shall:

- Review all alerts from the IDS in a timely fashion and report all confirmed events to Cybersecurity Ops, Engineering, & IAM via the Cybersecurity Incident Reporting process.
- Ensure those networks are routinely scanned for vulnerabilities and that vulnerabilities are remediated according to the appropriate institution's Vulnerability Management requirements.
- Monitor network traffic and log data, investigate, and, when appropriate, report anomalies as identified above.
- Students or sponsored users can assist in management of privately managed networks with oversight by a specific, named USNH employee.

Owners of privately managed networks must submit documentation to CS&N annually verifying their privately managed network still conforms with this standard. Network Administrators and/or CS&N can request an audit of any privately managed network, at any time, to confirm compliance.

PROHIBITED WITHIN PRIVATELY MANAGED NETWORKS

Privately managed network operators are prohibited from deploying wireless networks to ensure seamless uninterrupted service for all USNH centrally managed wireless networks.

University System of New Hampshire

FAILURE TO ADHERE TO THIS STANDARD

The Network System Administrators shall take **ALL** necessary steps to protect each USNH network from improperly configured or managed privately managed networks. At the discretion of the Network System Administrators, privately managed networks that exhibit the behaviors indicated below may be shut down, throttled, or otherwise impacted, if required to protect USNH or institutional information and information technology resources and/or to allow normal traffic and central services to resume on the impacted USNH network.

- Imposing an exceptional load on a campus service
- Exhibiting a pattern of network traffic that disrupts other services
- Exhibiting a pattern of malicious network traffic associated with scanning or attacking others
- Exhibiting behavior consistent with host compromise
- Failure to identify, investigate, and/or report a cybersecurity event occurring within the privately managed network

LEGACY NETWORK COMPLIANCE GRACE PERIOD

Any previously sanctioned Privately Managed Networks already connected to USNH Networks will be given a temporary compliance grace period. The intent of this temporary grace period is to allow the managers of each Privately Managed Network to work with Cybersecurity & Networking on:

- assessing existing security controls in those networks
- making any necessary security control improvements of modifications to bring those networks into compliance with this Standard
- certifying compliance of those networks
- or transitioning management of those networks to CS&N

As each Privately Managed Network will require differing levels of effort to achieve compliance, a grace period expiration date will be established for each Privately Managed Network after the security control assessment has been completed.

To maintain this status for the length of the established grace period, managers of Privately Managed Networks shall make a good faith effort to participate in the CS&N assessment process and address any mandatory improvements prior to the expiration date established for their network. Failure to do so may result in the Chief Information Security Officer (CISO) rescinding the compliance grace period for that Privately Managed Network. Loss of these protections prior to certification may result in a Privately Managed Network being shut down, throttled, or otherwise impacted.

University System of New Hampshire

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 shall 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* and will require certification of compliance with the requirements outlined above.

8 DEFINITIONS

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

- Access Control
- Availability
- Boundary Protection
- Confidentiality
- Exception
- Firewall
- Integrity
- Intrusion Detection System
- Protocol
- Privately Managed Network

- Remediate
- Risk
- Standard
- Vulnerability

9 ROLES & RESPONSIBILITIES

Network System Administrators:

- Set standards for network configuration, required network security elements, etc.
- Take action to protect the USNH Networks

Privately Managed Network Administrator:

- Ensures privately managed network segments are scanned for vulnerabilities as required in the appropriate institution's Vulnerability Management requirements
- Ensures vulnerabilities identified within privately managed network segments are remediated in line with the appropriate institution's Vulnerability Management requirements
- Monitors network traffic and log data
- Reviews all alerts from the IDS in a timely fashion
- Investigates anomalies on their network and all potential security events
- Reports all confirmed security events and anomalies to Cybersecurity Ops, Engineering, & IAM via the Cybersecurity Incident Reporting process
- Submits documentation to Cybersecurity Ops, Engineering, & IAM annually verifying privately managed network still conforms with this standard

Cybersecurity & Networking:

- Grants exceptions to this standard, including conducting assessments required for exception approval
- Audits privately managed networks

Cybersecurity Ops, Engineering, & IAM:

- Handles all cybersecurity event/incident investigation and response

10 RELATED POLICIES AND STANDARDS

- USNH Acceptable Use Policy
- USNH Cybersecurity Policy

University System of New Hampshire

- USNH Information Classification Policy
- Cybersecurity Exception Standard
- Vulnerability Management Standard

11 REFERENCES

- NIST SP 800-53 r4 SC-7: https://nvd.nist.gov/800-53/Rev4/control/SC-7
- NIST SP 800-53 r4 RA-5: https://nvd.nist.gov/800-53/Rev4/control/RA-5
- NIST SP 800-53 r4 AC-2: https://nvd.nist.gov/800-53/Rev4/control/AC-2

---

12 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:	01 MAY 2021
Approved by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, 16 OCT 2020 V2 UNH INFORMATION SECURITY COMMITTEE, 19 DEC 2019, v1.1
Reviewed by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, 10 JUL 2020, v1.1 USNH INFORMATION SECURITY COMMITTEE, JAN 2019, v1.1 UNH INFORMATION SECURITY COMMITTEE, 19 DEC 2019, v1.1
Revision History:	REVISED, CHIEF INFORMATION SECURITY OFFICER REVIEW, v1.2 REVISED, ELEVATE TO USNH STANDARD, R BOYCE-WERNER, 30 JAN 2020, v1.1 REVISED, UNH INFORMATION SECURITY COMMITTEE FEEDBACK, 19 DEC 2019, v1.1 DRAFTED, D CORBEIL, 20 NOV 2019 (Private Network Standard v1)