University System of New Hampshire

NETWORK SECURITY AND MANAGEMENT STANDARD

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

1. PURPOSE

Enterprise Technology & Services (ET&S) is charged by the University System of New Hampshire (USNH) to manage the campus communications networks efficiently. This standard establishes a framework of principles, guidelines, and operational procedures that ensure the effective and efficient management of the campus communications networks consistent with the mission and goals of USNH's educational institutions. The following provides information and guidelines for the responsible management and administration of the University System of New Hampshire's (USNH) communications networks.

2. SCOPE

This standard applies to USNH faculty, staff, students, volunteers, interns, and guests requiring access to electronic resources.

3. STANDARD

The campus communications networks (data, voice, video) are mission-critical resources that all campus community members utilize. Therefore, these resources must be managed effectively to ensure maximum availability, accessibility, and operational efficiency.

A. Security and Encryption

1. ET&S has the authority and responsibility to monitor the campus communications networks to ensure Confidentially, Integrity, and Availability of USNH information. Unless explicitly authorized by USNH ET&S Cybersecurity, any form of software that explores "sniffs" or probes the network for any reason is strictly prohibited. ET&S tests and investigates all actions or conditions that pose risks to network security and will take corrective and/or protective measures as necessary to ensure the continued proper function of the campus communications networks.

2. ET&S actively monitors the network for intrusion. Network Intrusion Detection and Presentation systems are deployed and monitored by ET&S staff. Any entity identified as a potential unfriendly host is immediately denied access to the campus network and reported to the proper authorities for further investigation and subsequent action.

3. ET&S manages and configures the Campus/Enterprise firewalls according to the guidelines contained within this policy. The Firewall Policy is reviewed yearly, and new rules are implemented with a risk analysis.

4. The guest wireless network is available for parents, vendors, and other guests of USNH that are on-campus to conduct business related to USNH and is only to be utilized in strict adherence to all USNH policies. The guest wireless network cannot directly access any non-public USNH resources. Information about access to the USNH guest wireless can be found at: https://td.unh.edu/TDClient/60/Portal/KB/ArticleDet?ID=3190

5. USNH networks shall be physically and logically segmented. Network segmentation is an architectural approach that allows USNH to divide a local area network into multiple segments or subnets, improving monitoring, performance, and enhancing security.

6. USNH uses sandboxes to test new applications that may contain viruses or cause compatibility issues with other systems. In addition, USNH conducts Research and Development projects, and ET&S ensures these networks are isolated safely from the USNH productions networks.

B. Network Hardware/Software (routers, switches, servers, other network devices)

1. The physical network standard on campus is exclusively Ethernet, IEEE 802.x. The wireless Ethernet strictly adheres to the 802.11x and 802.11g standards.

2. The connection of any network device (routers, switches, servers, other network devices) to the campus network without the prior knowledge and expressed permission of ET&S is prohibited.

3. The standardization of manufacturers for networking technology decreases integration problems and increases our ability to provide a flexible, robust, and integrated network providing optimal network connectivity and reliability. Standardization also provides seamless data integration, voice, and video and heightens the quality of service and network resilience. USNH has standardized the hardware and its supporting software for the wired and wireless networks. These standards are available from ET&S at: https://www.usnh.edu/it/departments/cybersecurity/technologycybersecurity-policies-standards

4. It is important to use enterprise-wide network protocols to allow integration, reliability, and help maintain simplicity in a large complex network as the enterprise evolves. Although other protocols are not strictly prohibited, the primary protocol supported on the USNH communications networks is TCP/IP using secure encrypted protocols such as https or sftp.

5. ET&S will centrally manage and keep logs for network equipment. Additionally, network technology administrators shall restrict access by the principle of least privilege and, when possible, enable multifactor authentication (MFA).

6. USNH change management policies will be followed for all configuration changes.

7. Critical security firmware/software patches will be coordinated and applied in accordance with the USNH change management policies.

C. Disaster Recovery - ET&S is responsible for maintaining, testing, and continuously improving a plan for recovery of the communications networks in the event of a disaster. Community members can find details in the ET&S Disaster Recovery Plan.

D. Device Registration and Address Allocation

1. Users shall register all hosts (computers) on the USNH network with an accurate and unique addressing scheme assigned by ET&S.

2. Faculty and staff needing help to connect a new device to the campus network should contact the ET&S Help Desk for assistance at: https://www.usnh.edu/it/need-it-help

3. Users may request a static address allocation by contacting the ET&S Help Desk. Requests for static addresses or creating a new network will be reviewed and acted upon as appropriate in the best interests of the campus network and the user community at: https://networking.usnh.edu/provision/

4. Domain registrations are managed by ET&S Networking Group and follow the USNH format (usnh.edu, keene.edu, plymouth.edu, unh.edu) for domain administration. Any request needs to be approved by ET&S.

5. A security scanning audit is periodically performed on all networked devices on the USNH networks to ensure hardening procedures are in place for security purposes.

E. Network Guidelines - The campus communications networks are a limited resource that exists to facilitate the goals and mission of USNH. Users may not infringe or encroach on the availability or use of the campus network by others. Examples of activities not allowed include (but are not limited to):

1. Using an IP address that has not been assigned or approved by ET&S.

2. Allowing a node or system on the network to become “open” to the extent that it is a target for hackers and a possible launching pad for an internal attack on the campus network or the Internet in general.

3. Monitoring or “sniffing” data on the network.

4. Flooding the network, either intentionally or unintentionally.

5. Running a commercial or for-profit service on the network.

6. Registering a system without using the usnh.edu or other USNH approved domains.

7. Establishing, enabling, or providing network services that interfere with the normal operation of the campus communications networks or users of the network or create security risk and exposure.

8. Installing Wireless Access Points.

9. Installing Firewalls other than software firewalls.

10. Installing Ethernet switches or routers.

11. Physical connections to the network will follow industry standards, such as EIA/TIA Standards for cabling, FOA Standard for Fiber Optics cabling, and IEEE 802.11X for wireless connections. Industry standards allow USNH to control costs, ensure compatibility, and use the latest security features.

4. VIOLATION OF THE STANDARD

Intentional or knowing violations of this standard may constitute misconduct. Accordingly, employees are subject to disciplinary action, up to and including suspension without pay and dismissal, in accordance with the pertinent employment policies for Staff and Faculty.

5. 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.

A community member may submit other requests here: Submit an IT Question.

---

6. DOCUMENT HISTORY

Effective Date: January 30. 2022
Drafted: Dave Yasenchock. January 15, 2022 v01
Revised, USNH Cybersecurity GRC Standards Committee, January 20, 2022
Reviewed by: Dr. David Yasenchock, Director Cybersecurity GRC, January 21, 2022
Approved by: Thomas Nudd, Chief Information Security Officer, January 29, 2022