University System

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 {ëăúŜY℡ă networks

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 C

5 MAINTENANCE OF PROCESSES AND PROCEDURES RELATED TO THIS STANDARD

As part of the mandatory annual review of this Standard required by the , 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 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

- 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)