University System of New Hampshire

Internet of Things (IoT) Usage Standard

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: Cybersecurity & Networking
Approved Distribution: Designated Reviewers Only
Status: In-Force

1 PURPOSE

The purpose of this standard is to provide guidelines and regulations for the responsible and secure use of Internet of Things (IoT) devices within the university campus to ensure the safety, security, and privacy of university community members and the integrity of university network infrastructure.

2 SCOPE

This standard applies to all university departments, units, employees, contractors, and third-party service providers who handle university data and information systems. An IoT device is defined by having an embedded operating system that does not support the installation of security agents such as antivirus and does not lend itself to frequent software updates. This includes devices such as printers, security cameras, smart speakers, smart lights, industrial controls, smart TVs, video streaming devices, personal network attached storage devices, VOIP phones, conference room systems, and digital signage.

3 AUDIENCE

All USNH community members who access USNH information technology resources should be familiar with this Standard.

4 STANDARD

4.1 Approval and Registration:

- All IoT devices intended for use within the university campus must be approved and registered with the university's IT department for "Network Registration."

- Registration should include device type, manufacturer, model, and purpose of use.

4.2 Security Measures:

- All IoT devices must adhere to the university's cybersecurity standards.
- Devices should have up-to-date firmware and security patches applied.
- Use strong, unique passwords for IoT devices, and change default passwords immediately upon setup.
- Where possible, disable any default accounts and create new custom accounts.
- Implement encryption protocols (e.g., WPA3) for wireless IoT devices.
- Regularly update and patch IoT devices to protect against known vulnerabilities.
- Define the required services of the IOT device and disable or uninstall any additional features that are not required.

4.3 Network Access:

- When feasible, IoT devices must connect to designated and segregated IoT network segments to prevent interference with the university's main network.
- Access to university network resources should be restricted to only necessary and authorized connections.
- Unauthorized IoT devices or those not meeting security standards (i.e., causing network related alarms) may be disconnected.

4.4 Privacy and Data Handling:

- Users are responsible for ensuring that personal and sensitive data collected by IoT devices complies with applicable laws, regulations, and university policies.
- IoT devices should minimize data collection to the extent necessary for their intended purpose.
- When disposing of IoT devices, ensure the secure deletion of data and proper disposal according to university procedures.

4.5 Physical Security:

- Users should physically secure IoT devices to prevent theft or tampering.
- Ensure devices are not blocking emergency exits or posing safety hazards.

4.6 Monitoring and Auditing:

- The university IT department reserves the right to monitor and audit IoT devices and network traffic to ensure compliance with this standard and identify security threats.

4.7 Incident Reporting:

- Users must report any security incidents, breaches, or unauthorized access related to IoT devices promptly to the university's IT department.

4.8 Guests and Visitors:

- Guests and visitors using IoT devices on campus should be informed of this standard and adhere to its guidelines.

4.9 Non-Compliance:

- Violations of this standard may result in the suspension of IoT device access privileges and disciplinary action.

4.10 Policy Review:

- This standard will be reviewed periodically to ensure its effectiveness and relevance.

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 Policy 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.

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:	October 23, 2023
Approved by:	Thomas Nudd, CISO
Reviewed by:	Dr David A Yasenchock, Director, Cybersecurity GRC
Revision History:	V 1.0