University System of New Hampshire

Computer/Information Technology Lab Standard

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

1. Purpose

This standard outlines the guidelines and regulations governing the use of computer labs within the university campus to ensure equitable access, maintain the security and integrity of university resources, and create a conducive learning and working environment.

2. Scope

This standard applies to all university departments, units, employees, contractors, and third-party service providers who handle university data and information systems.

3. Standard

3.1 Access Control:

- Access to computer labs is primarily for registered students, faculty, and staff. Visitors may use computer labs with prior authorization.
- Users or sponsors may be asked to present a valid university identification or visitor passes to gain access.

3.2 Hours of Operation:

- Computer labs will have designated operating hours, and users must adhere to these schedules.

3.3 Prioritization:

- Academic and research purposes take precedence over personal use during peak hours.

3.4 User Responsibilities:

- **Respect and Conduct:**
  - Users must conduct themselves in a respectful and courteous manner, refraining from disruptive behavior, harassment, or misuse of lab equipment.
- **Software and Data:**
  - Users are responsible for adhering to software licensing agreements and copyright laws.

  - Do not install, remove, or modify software on lab computers without authorization.
  - Save personal data to external or cloud storage system, such as one drive, etc. devices. The university is not responsible for data loss.
- **Security:**
  - Users must log out of computers when finished and report any suspicious activity to lab staff or the USNH IT Department (ET&S).
  - Do not share login credentials.
- **Cleanliness:**
  - Keep the lab environment clean and tidy, disposing of trash properly.
  - Report any damage or equipment issues to lab staff promptly.
- **Food and Drink:**
  - Food and drinks near IT equipment is prohibited in computer labs to prevent damage to equipment.

3.5 Lab Equipment:

- **Equipment Use:**
  - Priority use for lab equipment is for academic and research-related tasks.
  - Report malfunctioning equipment to lab staff immediately.
- **Printing:**
  - Follow university printing policies and guidelines.
  - Do not waste paper or supplies.

3.6 Network and Internet Use:

- **Network Access:**
  - Priority use for the university network is for academic, research, and administrative purposes.
  - Unauthorized access to the network or tampering with network settings is prohibited.
- **Bandwidth Usage:**
  - Try to avoid excessive bandwidth usage for non-academic purposes during peak hour, such as music videos or movies that are for non-academic purposes.

3.7 Privacy and Data Security:

- **Data Privacy:**
  - Respect the privacy of others and do not access or attempt to access their files or data without permission.
- **Personal Devices/Workstations:**

- Do not connect personal workstations to the lab wired lab network without ET&S authorization. Consider using the USNH wireless network for personal devices.

3.8 Security and Compliance:

- **Security Awareness:**
  - Complete annual security awareness training sessions provided by the university.
- **Non-Compliance:**
  - Violations of this policy may result in loss of lab access privileges and disciplinary action.

4. Exceptions

Requests for exceptions to this Standard shall be submitted and approved according to the requirements provided in the Cybersecurity Exception Standard.

5. Enforcement

Anyone found to have violated this policy may be subject to disciplinary action, up to and including suspension of access to institutional resources or termination of employment. Students may be referred to Student Affairs for discipline. A violation of this policy by a temporary worker, contractor or vendor may result in action up to and including termination of their contract or assignment with USNH.

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 a comprehensive list of all Policies and Standards, visit the USNH Cybersecurity Policies & Standards page.

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:	February 2, 2024

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