1. Purpose

The University System of New Hampshire (USNH) is committed to maintaining the security and confidentiality of institutional data. The purpose of this standard is to prevent unauthorized access, damage, or threats to the security of USNH resources, and to establish procedures for USNH community members to obtain authorized access when necessary.

2. Scope

This Standard applies to all USNH community members granted access to institutional information, information technology resources, and controlled USNH areas. Controlled USNH areas are areas identified in a facility or location that requires limited access, a higher degree of protection, or that stores sensitive, protected, or restricted information. For more information on data classification, please refer to the Information Classification Policy.

3. Audience

All USNH community members should be familiar with this Standard.

4. Standard

Physical access to controlled areas shall be limited to authorized personnel who require access to fulfill designated responsibilities. Supervisors and managers of controlled USNH areas are responsible for documenting policies and procedures to prevent unauthorized access. USNH data stewards and community members shall manage university data in accordance with the guidelines set forth in this policy and other university rules governing data classification, storage, access, and disposal.

4.1 Physical Access

The following physical security measures apply to help protect USNH resources and facilities:

- Entrances/exits and windows of controlled areas shall be locked when unattended and protected by electronic security systems, security cameras, and/or physical access devices (i.e., keys, badges, card readers).
- Physical access devices shall be secured when not in use. If physical access devices are lost or stolen, it shall be reported immediately to ET&S Cybersecurity or the University police.
- Never loan or share physical access devices and/or mechanisms, including access codes, passwords, and badges with anyone.
- Physical access devices and/or lock combinations shall be updated regularly and in response to personnel changes.
- Never allow unauthorized individuals to enter a controlled location. An unauthorized person refers to any person who does not have permission to access a controlled area, system, or data.
- Prevent “tailgating,” which occurs when an unauthorized person follows an authorized person into a controlled area. For example, do not hold the door open for an unknown person if a building requires a physical access device for entry.
- Physical data classified as sensitive, protected, or restricted according to the USNH Information Classification Policy shall be restricted to authorized personnel and securely stored, such as in a locked file cabinet, locked office, or a safe. This includes Controlled Unclassified Information (CUI) created or owned by the government such as DoD critical security information.
- Report any suspicious activity to the University Police or by calling 911 if it is an emergency.
- In the event of a data breach, the CISO, in cooperation with the USNH General Counsel’s Office, shall manage all required notifications to relevant regulatory bodies pursuant to the relevant standard(s) (see Cybersecurity Policy 5.14.3).

To effectively authorize physical access to controlled areas, the following shall be implemented by the designated authority for each department or institution:

- Ensure that any access granted to an individual is the minimum access necessary to perform job responsibilities.
- Develop, review, and routinely update a list of individuals with authorized access to controlled areas, such as those with physical access devices.
- When access is no longer required (i.e.: retirement, termination, lost access device), immediately make necessary changes.
- Maintain physical access audit logs for a minimum of thirty days to monitor controlled areas.

4.2 Visitor Access

Individuals not regularly authorized to access controlled areas are considered visitors. The following requirements apply to visitor access:

- Visitor access authorizations shall be approved by the designated authority for each department or institution.
- Authorized visitors shall be escorted by staff members when accessing controlled areas.
- Visitor access to controlled areas shall be logged, reviewed periodically, and maintained for a minimum of thirty days.
- Access logs shall include the visitor’s name, date of access, entry/Departure times, the visitor’s employer (if applicable), reason for visit, the visitor’s signature, and the name of the individual accompanying the visitor.
4.3 Physical Data Handling Procedures

Departments shall establish procedures to ensure physical data is handled based on its classification and according to the Information Classification Policy. The classification of data is the responsibility of data stewards, who can provide information on classification requirements involving regulated data within their subject matter area. Identifying and classifying data is critical to determine the appropriate degree of protection.

Some general responsibilities for all USNH community members are as follows:

- Practice a “clean desk policy”- secure non-public documents so they are never left unattended and at risk of unauthorized access (i.e., lock in a cabinet, do not leave on a printer).
- Whenever possible, review documents containing non-public information electronically and refrain from printing them out.
- University data should only be stored on or connected to institutionally owned devices and approved University applications.
- Dispose of physical data securely when it is no longer needed or required by applicable legal and regulatory standards. Printed protected information must be disposed of using a crosscut shredder or an approved shredding service.
- Please contact ET&S or the appropriate institutional data steward for additional guidance to determine a department’s policy on secure disposal.
- Report unauthorized access, use, disclosure, modification, or destruction of data immediately.

4.4 Environmental Controls

Adequate controls shall be implemented to protect against and plan for the possibility of environmental hazards. Reasonable attempts must be made to protect facilities and systems from hazards such as fires, water damage, extreme temperatures, or power outages.

5. Monitoring and Reporting

All members of USNH are responsible for maintaining the security of USNH facilities and data. Violations of security policies must be reported immediately.

6. 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.
7. Definitions

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

- Access
- Access Control
- Authorization
- Controlled Areas
- Least privilege
- Log
- Physical Security

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

<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>December 23, 2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved by:</td>
<td>Dr David A Yasenchock, Interim CISO</td>
</tr>
<tr>
<td>Reviewed by:</td>
<td>Dr David A Yasenchock, Director, Cybersecurity GRC</td>
</tr>
<tr>
<td>Revision History:</td>
<td>V 1.00 REVISED, K Sweeney, 14 APRIL 2023</td>
</tr>
</tbody>
</table>