University System of New Hampshire

Physical and Camera Security Standard

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: ET&S Cybersecurity GRC
Approved Distribution: PUBLIC
Status: IN FORCE

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. It also outlines procedures for authorized access and covers the setup and operation of a uniform camera security system at USNH. As needs shift and technology advances, this document will continuously evolve to match the University System's requirements.

2. Scope

This Standard applies to all USNH staff, faculty, students, affiliates, and controlled USNH areas. Controlled areas refer to spaces in facilities necessitating limited access, heightened protection, or storage of sensitive data. For data classification specifics, consult the Information Classification Policy. Furthermore, this Standard covers security cameras across USNH sites, campuses, off-campus structures, and USNH-owned or controlled properties.

3. Standard

3.1 Physical Access

Physical access to controlled areas shall be limited to authorized personnel who require access to fulfill designated responsibilities. Area supervisors and managers are responsible for documenting policies and procedures to prevent unauthorized access. USNH students, staff, faculty, and affiliates shall manage university data in accordance with this Standard and University rules governing data classification, storage, access, and disposal.

3.1.1 Physical Security Measures

The following physical security measures apply to help protect controlled USNH areas:

3.1.1.1 Entrances/exits and windows of controlled areas shall be locked when unattended and protected by electronic security systems, cameras, and/or physical access devices (I.e., keys, badges, card readers).

3.1.1.2. Secure physical access devices when not in use. Lost or stolen devices must be promptly reported to ET&S Cybersecurity or University police.

3.1.1.3 Never share physical access devices and/or mechanisms, including codes, passwords, and badges.

3.1.1.4 Physical access devices and/or lock combinations shall be updated regularly and in response to personnel changes.

3.1.1.5 Restrict access to sensitive, protected, or restricted physical data, storing it securely (locked file cabinets, offices, safes). This includes Controlled Unclassified Information (CUI) created or owned by the government such as DoD critical security information.

3.1.1.6 Prevent unauthorized access and "tailgating" (unauthorized person following authorized person) by not holding doors open for unknown individuals.

3.1.1.7 Report suspicious activity to the University Police or by calling 911 in an emergency.

3.1.1.8 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 the *USNH Cybersecurity Policy* 5.14.3).

3.1.2 Physical Access

The designated authority in each department or institution should ensure effective authorization for physical access to controlled areas by:

3.1.2.1 Granting only minimum necessary access for job duties.

3.1.2.2 Developing, reviewing, and regularly updating a list of authorized individuals, including those with physical access devices.

3.1.2.3 Promptly adjusting access when no longer needed (retirement, termination, lost access device).

3.1.2.4 Maintaining physical access audit logs for at least thirty days to monitor controlled areas.

3.2 Visitor Access

3.2.1 Visitor Access Requirements

Individuals not regularly authorized to access controlled areas are considered visitors. Visitor access must adhere to the following:

3.2.1.1 Approval of visitor access by department or institution authority.

3.2.1.2 Authorized visitors shall be accompanied by staff members in controlled areas.

3.2.1.3 Logs of visitor access shall be maintained for at least thirty days and reviewed periodically.

3.2.1.4 Access logs shall contain visitor's name, date of access, entry/departure times, employer (if applicable), visit reason, signature, and the accompanying individual's name.

3.3 Physical Data

3.3.1 Physical Data Handling Procedures

Departments establish data handling procedures based on its classification and 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.

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

3.3.1.1 Practice a "clean desk policy"- secure non-public documents so they are never at risk of unauthorized access (i.e., lock in a cabinet, do not leave on a printer).

3.3.1.2 Whenever possible, prefer electronic review over printing.

3.3.1.3 Store University data on institutionally owned devices and approved applications.

3.3.1.4 Securely dispose of data when it is no longer needed or required by applicable legal and regulatory standards. For example, use a cross-cut shredder or an approved shredding service.

3.3.1.5 Contact ET&S or the appropriate data steward for additional guidance to determine a department's disposal policy.

3.3.1.6 Report unauthorized access, use, disclosure, modification, or destruction of data immediately.

3.4 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.

3.5 Camera Security

3.5.1 Camera Security System Roles and Responsibilities

Camera system oversight protocols differ across USNH. Any department, facility owner, or office seeking to install and utilize security cameras shall initiate the process and obtain approval by submitting a formal request to the Campus Safety department or University Police. The installation of security cameras shall be the financial responsibility of the requesting school, department, or office, and all camera installations are subject to federal and state laws.

3.5.1.1 All video security camera installations shall be centrally documented and approved by Campus Safety or University Police.

3.5.1.2 Campus Safety or University Police shall review and approve all requests for security cameras before any work is completed or funds are expended.

3.5.1.3 Campus Safety or University Police shall have full access to view live/stored security camera images that are subject to this standard, if needed.

3.5.1.4 USNH Cybersecurity shall annually review and update technical specifications and pre-certify vendors with USNH Procurement for approved camera system equipment and protocols.

3.6 Camera Requirements Technical Standards for Camera Systems

3.6.1 Technical Standards and Requirements for Camera Systems

Only USNH Cybersecurity and Campus Police approved vendors shall be used to provide and install security cameras. Technical requirements for camera systems include:

3.6.1.1 The camera system shall meet the minimum standard for short-term storage of 30 days and for long-term storage for sensitive data used in disciplinary or criminal investigations. Cameras must also conform to the specifications as outlined in the Vendor Installation Requirements provided upon approval.

3.6.1.2 Cameras shall be a non-federally banned but technically acceptable model, Wisenet WAVE compliant, and approved by Cybersecurity.

3.6.1.3 Cameras shall have a minimum resolution of 1080P (1920x1080 pixels).

3.6.1.4 Camera shall be capable of "edge recording," which allows for local SD card recording as a backup in case of network outages.

3.6.1.5 All cameras shall have IP66 (Weatherproof) Rating.

3.6.1.6 All cameras shall meet the PoE/PoE+ power requirements set forth by USNH Telecom.

3.6.1.7 Video data from security cameras shall be stored in approved ET&S storage centers and intended to be used only for safety, law enforcement, personnel action and/or student conduct purposes.

3.6.1.9 No audio recordings shall be made using the security cameras; audio recording capability shall be disabled when a camera is installed.

3.6.1.10 Security video data shall not be provided to any non-university entity unless it is required for criminal investigations and will only be provided internally for disciplinary or criminal investigations as requested and approved by USNH Cybersecurity, USNH General Council and University Police or Campus Safety.

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.

DOCUMENT HISTORY

Effective Date:	28 AUGUST 2023
Approved by:	CHIEF INFORMATION SECURITY OFFICER, T NUDD, 28 AUGUST 2023, V1
Reviewed by:	CHIEF INFORMATION SECURITY OFFICER, T NUDD, 28 AUGUST 2023, V1 DIRECTOR, CYBERSECURITY GRC, DR DAVID A YASENCHOCK, 28 AUGUST 2023, V1
Revision History:	