USNH Public Safety Video Camera System Standard

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: Cybersecurity Governance Risk and Compliance (GRC)
Approved Distribution: PUBLIC
Status: IN FORCE

1. Purpose
Per directive of the UNH Vice President for Finance and Administration / Chief Financial Officer and the UNH Chief of Police / Associate Vice President for Public Safety and Risk Management (VP of Public Safety), a working group was previously established in 2010 to develop standards, policies and procedures for cost-effective, coordinated standardization of a University of New Hampshire campus security camera architecture and infrastructure. The group is tasked with recommending policy and practice that is consistent, coordinated, cost-effective and technologically sound and which establishes a protocol for compliance with all state and federal laws.

This document summarizes the existing standards and procedures related to establishing and operating a standardized security system infrastructure at USNH. It is a living document and it evolves as the needs of the University System and security camera technologies change. Users who need to install security cameras must obtain approval from the VP of Public Safety and fill out the form at https://td.unh.edu/TDClient/60/Portal/Requests/ServiceDet?ID=174 to request further guidance.

2. Scope
This standard applies to video security cameras that are installed at the University System of New Hampshire. This standard applies to all University System campuses and off-campus buildings, or property owned or controlled by the University of New Hampshire and any user who is requesting for a camera to be placed as needed.

New installations and cameras must comply with this standard. Existing cameras and installations shall migrate to comply with this standard when replaced, upgraded, or sooner if otherwise appropriate.

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

4. Authority
This Public Safety Video Camera System (PSVCS) Standard is interpreted by the UNH VP of Public Safety, representing the authority of the CFO. The VP of Public Safety leads the working group and approves deployment of security cameras.

Effective Date: April 18, 2023
Drafted: Colin Grebloski/Carl Nickerson March 13, 2023
Revised: Colin Grebloski April 18, 2023
Reviewed by: Dr. David Yasenchock, Director Cybersecurity GRC, April 18, 2023
Approved by: Thomas Nudd, Chief Information Security Officer, April 18, 2023
5. STANDARDS

1. All video security camera installations will be centrally documented and retained by USNH Cybersecurity.

2. The VP of Public Safety reviews and approves all initial requests for security cameras before any work is completed or funds are expended.

3. The Campus Police Department will have full access to view live security camera images and stored images for all cameras that are subject to this standard.

4. Signs will be installed in all areas where security cameras are installed informing the public that video is being recorded. Exceptions to the sign requirement may be made if such signs would defeat the camera’s purpose and must be approved in writing by the VP of Public Safety after consultation with the USNH General Counsel. Video data from security cameras will only be stored in approved ET&S storage centers and is intended to be used only for safety, law enforcement, personnel action and/or student conduct purposes.
   - The operation for long-term storage of images is centrally funded and operated by ET&S.

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

6. Access to cameras shall be granted by ET&S following a “zero trust security architecture” to maintain security standards and following a defined classification.
   - Classification follows as:
     - View only,
     - View and search,
     - View, search and copy,
     - Administrative.
   - Access will be granted on a need-only basis through submission to USNH Cybersecurity.
   - 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 or the VP of Public Safety.

7. Only vendors approved specifically by USNH Cybersecurity for these purposes will be used to provide and install security cameras.

8. The camera system must 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.

9. Cost responsibility for security camera acquisition and installation is as follows:
   - Cameras and camera installation, maintenance, repair, replacement – Client/department
   - Ethernet port(s), recurring charges and required infrastructure work – Client/department
   - Secure network operation – USNH ET&S
   - License for accessing central servers – Client/department
   - License renewals for accessing the central server – USNH ET&S
10. To report security camera service disruptions (other than the camera itself):
   - During customary work hours, call the ET&S Help Desk at (603) 862-4242.
   - Any other time, call UNH Police Dispatch at (603) 862-1427.

USNH Security Camera Working Group

1. The working group is chaired by the VP of Public Safety.
2. At a minimum the working group includes representatives from USNH CyberSecurity, USNH Telecom, USNH ET&S, Facilities and Business Affairs. Other departments may be represented as desired by those departments or as required by the VP of Public Safety.
3. The working group makes recommendations to the CFO for establishment and annual review of the applicable standard and procedures.
4. If deemed necessary (after consideration of other safety and security practices), the VP of Public Safety requests that the Working Group review and provide technical assistance as appropriate.
5. USNH Cybersecurity, in coordination with USNH Procurement, vets and pre-certiﬁes a list of approved vendors and equipment for camera systems and communications protocols which must be used.
6. USNH Cybersecurity shall determine the technical standards and speciﬁcations of the camera system based on operational needs and changes to technology over time. Cybersecurity shall review and update these speciﬁcations annually.
7. The working group will maintain, update and provide to approved camera requestors a typical cost sheet that will unitize known and predictable costs. It is understood that the installation, electrical services, communication services, physical location requirements, choice of cameras and special needs of clients impact the cost and cannot be predicted without formal quotes from service providers.

Procedure for Installing One or More Security Cameras:

1. Users requesting the installation of security cameras must fill out a web request form at https://td.unh.edu/TDClient/60/Portal/Requests/ServiceDet?ID=174.
   - Clients must have the approval of the relevant director or dean, at a minimum, to request installation of security cameras.
2. Client should specify area(s) where camera(s) are to be installed.
3. Cybersecurity provides client a copy of this document and provides further guidance.
4. VP of Public Safety reviews the request from the client, approves, and/or references the request back to ET&S for detailed technical discussion.
5. The project is then referred to Facilities Control Center for project manager assignment (if size warrants).
   - For smaller installations the client department may choose to provide their own project manager. The project manager is not required to have deep technical knowledge, but must remain informed about all
phases of the quoting, design and installation, provide funding for the project, and represent the leadership of the client department.

6. Project manager requests a camera installation quote from an USNH Cybersecurity-approved vendor
7. Vendor will identify additional work that is required from other trades as needed, including:
   a. Electrical service, if needed
   b. Ethernet port(s)
   c. Conduit
8. Project manager requests infrastructure preparation from appropriate USNH service units/trades, if needed.
9. Camera Vendor supplies Project manager with a quote for server camera licenses.
10. Project manager
    a. Schedules access to the installation location with the client.
    b. Coordinates installation date with Vendor and IT.
11. Vendor installs and configures cameras consistent with the Vendor Installation Requirements.
12. The client is responsible to identify users that may require access to relevant camera footage.
    a. Client shall submit a service request through the IT Accounts Management System at https://accountsmanagement.unh.edu. Cybersecurity authorizes appropriate user accounts for the client on the central server (2 maximum personnel).
13. Cybersecurity provides client software installation support and basic usage training for client.
14. Project manager informs UNH Police that the cameras are ready to be viewed as agreed above.
15. USNH ET&S, Cybersecurity and Client approve/sign off on the installation.

CAMERA TECHNICAL STANDARDS AND REQUIREMENTS:

1. Cameras shall be a non-federally banned but technically acceptable model that is Wisenet WAVE compliant and approved by Cybersecurity.
2. Camera shall be capable of a minimum resolution of 1080P (1920x1080 pixels).
3. Camera shall be capable of “edge recording”, which allows for local SD card recording as a backup in case of network outages.
4. All cameras shall have IP66 (Weatherproof) Rating.
5. All cameras shall meet the PoE/PoE+ power requirements set forth by USNH Telecom.

DOCUMENT HISTORY

<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>April 18, 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved By:</td>
<td>Thomas Nudd, Chief Information Security Officer, April 18, 2023</td>
</tr>
<tr>
<td>Reviewed By:</td>
<td>Dr. David Yasenchock, Director Cybersecurity GRC, April 18, 2023</td>
</tr>
<tr>
<td>Revision History:</td>
<td>Colin Grebloski April 18, 2023</td>
</tr>
</tbody>
</table>