SEC-034

Use of University Networked Cameras that View University Assets and Public Spaces

Effective Date Monday, April 6, 2015

Status Final

Last Revised Monday, July 24, 2023

Policy Type University

Contact Office
Safety & Security (Department of)

Oversight Executive
Executive Vice President and Chief Operating Officer

Applies To
Academic Division The Medical Center

Table of Contents

Reason for Policy

Networked cameras that view University assets and public spaces are to be installed, maintained, and monitored to enhance safety and security while respecting the privacy expectations of members of the University community.

Definition of Terms

Internal Use Data

Data that is typically a public record available to anyone by the Virginia Freedom of Information Act (FOIA) but is also not intentionally made public (see the definition of **public data**). Examples may include salary information, contracts, and specific email correspondence not otherwise protected by a FOIA exemption. For a complete list, see Code of Virginia § 2.2-3700 Virginia Freedom of Information Act.

Public Data

Data intentionally made public and are therefore classified as not sensitive. Any data that are published and broadly available are, of course, included in this classification. University policy holds that the volume of data classified as not sensitive should be as large as possible because the widespread availability of such information will enable others to make creative contributions in pursuit of the University's mission.

Public Record

Any writing or recording — regardless of whether it is a paper record, an electronic file, an audio or video recording or any other format — that is prepared or owned by, in possession of a public body or its officers, employees, or agents in the transaction of public business. Freedom of Information Act. All public records are presumed to be open and may be withheld only if a statutory exemption applies.

Networked Camera

A camera used or potentially used for monitoring and recording public areas to enhance the safety and security of people and property, discourage criminal activity, and investigate incidents of alleged policy or criminal violations.

Networked Camera Monitoring

Viewing camera feeds in real-time.

Networked Camera Oversight Group

The University group charged with oversight of the Networked Camera System and hearing appeals related to camera requests, composed of representatives from these areas: Safety and Security (including the Director of Safety & Security Systems and Technology as an ex-officio member); Executive Vice President & Provost; Student Affairs; either the Law School, Darden School, or the Medical School; Information Technology Services; University Architect; Facilities Management; and Medical Center Facilities and Safety.

Networked Camera Recording

A digital or analog recording of a feed from a networked camera.

Networked Camera System

Video management software, network recorders, network switches, fiber, and category cable that create a system to view, record, and retrieve video from attached cameras.

Private Areas

Areas including but not limited to non-common areas of residence halls, bathrooms, shower areas, locker and changing rooms, and other areas where a reasonable person might change clothes. Additionally, areas dedicated to medical, physical, or mental health therapy or treatment are considered private areas unless regulatory requirements mandate otherwise.

University Facility

Any defined space of the University, including a room, lab, series of labs, building, or controlled outdoor area.

University Property

Land or buildings that the University owns or leases and that is under the control of the Board of Visitors. University property also includes premises the University uses for activities of its offices, departments, personnel, or students.

Policy Statement

Before purchasing any networked camera for installation in a University owned, leased, or operated facility to view public or private areas, regardless of cost, approval must be granted by the Director of Safety & Security Systems and Technology. An appeal to the decision made by the Director of Safety & Security Systems and Technology will be made to the Networked Camera Oversight Group with final authority being the Associate Vice President (AVP) for Safety and Security/Chief of Police. The requirements for installing and managing all networked cameras that view University assets and public spaces in University facilities and on University property are outlined below. Also included are requirements for the management, viewing, retention, dissemination, and destruction of any associated media and records by the regulations of the Virginia Public Records Act 42.1-76 et seq. of the Code of Virginia.

This policy does not imply or guarantee that cameras will be monitored in real-time 24 hours a day, 7 days a week.

Exceptions: This policy does not apply to:

1. Use of cameras solely for:
    - Remote monitoring of facility construction and progress.
    - Videotaping of athletic events or practices for reviews.
    - Carrying out human subject and animal research (which use is governed by University policies for research) or other legitimate educational purposes.
    - Monitoring a patient for clinical or behavioral reasons.

2. Use of cameras (whether stationary, body-worn, portable, or mobile) for:
    - Covert operations conducted by law enforcement during criminal surveillance.
    - Investigative or other law enforcement functions.
    - Parking enforcement or revenue collection.

1. **Authority:**
   Oversight of the design, installation, maintenance, and utilization of networked cameras and associated policies, standards, and procedures lies with the Department of Safety and Security (DSS) and the Networked Camera Oversight Group. This includes:
    - Design, maintenance, and review of a University strategy for the procurement, deployment, and use of networked cameras, including this and related policies.
    - Design and approval of University standards for networked cameras and their use.
    - Creation of the standard University networked camera system or service.
    - Authorization of the placement of all networked cameras.
    - Approval of the purchase of any new networked camera systems.
    - Review of existing networked camera systems and installations and identification of modifications required to bring them into compliance with this policy.
    - Creation and approval of procedures for the use of networked cameras.

2. **Networked Camera Placement:**

- The Department of Safety and Security maintains oversight of temporary or permanent networked cameras on Grounds. As such, all installations must be approved by DSS.
- All networked camera equipment must comply with University standards and be connected to the University's network.
- Departments and schools desiring the installation and use of networked cameras must complete a request for such installation in consultation with the Department of Safety and Security via the on-line Networked Camera Installation Request Form.
- All requests for networked cameras must include the location for the camera placement for the University facility or public space(s) and identify a funding source for the purchase and maintenance of the cameras.
- A Department of Safety and Security team member will follow up with the requester within 10 business days of receipt to schedule either a site-visit or otherwise collect the information needed for the Director of Safety & Security Systems and Technology to review the request.
- The Director of Safety & Security Systems and Technology will review the request and either approve or deny the request.
- Upon approval by the Director of Safety & Security Systems and Technology, the Department of Safety and Security coordinates with the department/school and oversees all activities associated with completing the request.
- The use of networked cameras is limited to public areas. Video surveillance conducted in private areas owned or controlled by the University must be authorized by the AVP for Safety & Security/Chief of Police.
- Networked cameras must not be directed at the windows of any privately-owned home not located on University property. Pan Tilt Zoom (PTZ) cameras that can view windows of privately-owned homes must be able to "mask" these windows by utilizing prohibitive software designed to prevent viewing. (Home in this context refers to any dwelling (rented, leased, or university property) where a person or persons reside either permanently or temporarily.)
- Networked cameras authorized in private areas will be used narrowly to protect persons, money, real or personal property, documents, supplies, equipment, or pharmaceuticals from theft, destruction, diversion, or tampering.
- Inoperative, placebo, or "dummy" networked cameras must not be installed or utilized, as they may lead to a false sense of security that someone is monitoring an operational camera.
- If the Director of Safety & Security Systems and Technology denies the request, the requesting department/school, program, contractor, or University organization may seek approval of their department/school vice-president/dean or chief executive officer, who may appeal the decision to the AVP for Safety & Security/Chief of Police.
- Removing cameras without authorization from the Director of Safety & Security Systems and Technology, the AVP for Safety & Security/Chief of Police, and the Networked Camera Oversight Group is prohibited.

3. **Camera Monitoring and Access to Recordings:**
    - ***Monitoring:*** University cameras are not monitored continuously under normal operating conditions but may be monitored by University Police or other authorized personnel for legitimate safety, security, or operational purposes that include but are not limited to: monitoring restricted access areas/locations, monitoring traffic for special events, managing visitors, conducting investigations of alleged policy or criminal violations, and enhancing the response of public safety agencies such as police, fire, and emergency medical services.
    - ***Access:*** The University Police will review all requests regarding the release or review of recorded video. Release or review of recorded video images will not occur without authorization by UPD and by the law, and when appropriate, consultation with University Counsel.

4. **Appropriate Use and Confidentiality:**
    - Video monitoring for security purposes is conducted professionally, ethically, and legally. Monitoring individuals based on characteristics of race, gender, sexual orientation, disability, or other protected characteristic is prohibited.
    - All faculty and staff are prohibited from using or disseminating information acquired from University cameras except for official purposes. All information and observations made while operating cameras are considered internal use data. This data can only be used for authorized University and law enforcement purposes or as the law requires. University Counsel will have access to the recordings as needed and requested.
    - Sharing of user credentials and passwords for camera access is strictly prohibited.
    - The Vice President & Chief Human Resources Officer (or designee) must approve using camera recordings as evidence in situations involving personnel policy infractions.
    - The use of camera recordings for any purpose not detailed within this policy is subject to review by the Department of Safety and Security.

5. **Training:**
    - UPD Camera Control Operators must receive regular training in appropriate camera use's technological, legal, and ethical parameters.
    - All other individuals granted camera access must be given a copy of this policy and provided with the appropriate level of training necessary.

6. **Storage, Retention, Disposal of Recordings, and Maintenance:**
    - Storage, retention, and disposal of recordings adhere to the regulations of the Virginia Public Records Act 42.1-76 et seq. of the Code of Virginia.
    - Recorded video is stored no less than 14 days. When retained as part of a criminal investigation or court proceeding, or other bonafide use as approved by the AVP for Security & Safety/Chief of Police (or designee) and the University Records Officer, retention may be longer.

7. **Responsibilities:**

    The ***Department of Safety and Security*** is responsible for:
    - Convening the Networked Camera Oversight Group as necessary.
    - On-going enterprise networked camera maintenance, assessment, and placement.
    - Collaborating with departments/schools to implement networked camera recommendations.
    - Coordinating the system design, purchase, operation, management, and monitoring of networked cameras pursuant to this policy.
    - Assessing new camera locations in coordination with Information Technology Services, UVA Medical Center, the Office of the Architect, Office of Facilities Management, and other stakeholders.
    - Developing and overseeing a preventative maintenance schedule to assure cameras remain in working order.
    - Developing and overseeing a system to recognize inoperable cameras.

    Information Technology Services is responsible for:
    - Maintaining a separate virtual network for the video management system.
    - Enabling networking for camera locations as needed.
    - Maintaining and updating software and firmware of virtual servers and storage arrays that are the foundational components of the video management system.

    The Office of the Architect is responsible for:

- Assessing new camera locations in coordination with the Networked Camera Oversight Group.
- Assisting in the installation and maintenance of cameras as needed for the preservation of architectural standards.

Departments Using the Video Management System are responsible for:

- Designating a camera oversight representative to liaison with Safety and Security.
- Identifying those individuals within their department that should have access to view cameras.
- Maintaining installed cameras in coordination with the Department of Safety and Security.
- Complying with this policy.

University faculty, staff, and Medical Center Employees are responsible for:

- Reporting any person who tampers with or destroys video cameras or equipment to the University Police Department.

The Office of Facilities Management is responsible for:

- Assisting in the installation of cameras as needed.
- Facilitating compliance with this policy in coordination with subcontractors.

8. **Compliance with Policy:**
   Failure to comply with the requirements of this policy may result in disciplinary action up to and including termination and expulsion in accordance with relevant University policies.

   Anyone who tampers with or destroys video cameras or equipment (including hacking, intercepting, interrupting, or interfering with service) is subject to criminal prosecution and University action, as applicable.

   Questions about this policy should be directed to the Department of Safety and Security.

Procedures

Complete the online Networked Camera Installation Request Form requesting an assessment of the proposed installation.
(Note: A member of the Department of Safety and Security will be in contact regarding the request within 10 business days of receipt of the request.)

Related Information

HRM-014: Standards of Conduct for University Staff Employees
HRM-050: Protection of Minors and Reporting Abuse
IRM-012: Privacy and Confidentiality of University Information
IRM-017: Records Management
Disciplinary Suspension or Termination of Academic Faculty

Medical Center Standards of Conduct:
Health System Policy BEH-001 ASPIRE Values
Medical Center Policy 0283 Behavioral Code of Conduct
Medical Center Policy 0291 Code of Conduct for Providers Who Hold Clinical Privileges
Medical Center HR Policy HR701 Employee Standards of Performance and Conduct

Major Category Safety, Security and Environmental Quality

Next Scheduled Review Friday, July 24, 2026

Revision History
Revised 7/24/23, 9/11/19, 6/27/17. Updated 5/6/2015.

Applies To Text
Academic Division and the Medical Center.

Supercedes Policy Text
XI.E.1: Use of Surveillance Cameras.

Last modified March 12, 2024 - 10:35am

Approved By Policy Review Committee

Approved Date June 27, 2017 - 12:00pm