Edit Policy

# SEC-034: Use of University Networked Cameras that View University Assets and Public Spaces

Date: 04/06/2015 Status: Final Last Revised: 06/27/2017
Policy Type: University
Contact Office: Police Department (University), Emergency Management (UVA)
Oversight Executive: Executive Vice President and Chief Operating Officer
Applies To: Academic Division and the Medical Center.
Table of Contents:

Policy Statement

1. Authorization and Installation
2. Placement of Cameras
3. Access and Camera Monitoring
4. Appropriate Use and Confidentiality
5. Training
6. Storage, Retention, Disposal of Recordings and Maintenance
7. Exemptions
8. Responsibilities
9. Compliance with Policy

Procedures



Reason for Policy:
The University endeavors to provide a safe and secure environment for members of the community by integrating camera technology and best practices that enhance safety and security while recognizing a reasonable expectation of privacy. The University has established regulations for the installation and use of cameras that view University assets and public spaces.

Cameras used to monitor a patient for clinical or behavioral reasons are covered by Medical Center Policy 0030.

Historically, Internet Protocol (IP) and analog video cameras have been installed in and around the University by various departments for legitimate purposes other than security. These cameras can often serve their intended purpose and supplement existing security cameras. Identifying and regulating the installation of all cameras that view University assets and public spaces allows the University to minimize the number of cameras that are installed in and around the University, and responsibly deploy its resources to enhance public safety.

Definition of Terms in Statement:

- Camera Monitoring:
  Viewing camera feeds in real-time.

- Camera Oversight Group:
  The University group charged with the oversight of the camera requests and approvals. It shall be composed of directors/managers of The Office of the Provost, Health System Environment of Care, Information Technology Services, University Police Department and University Office of Safety and Emergency Preparedness.

- Camera Recording:
  A recording of an analog video signal or recording a digital video stream from an IP camera.

- Controlled Data:
  Data that is a public record available to anyone in accordance with the Virginia Freedom of Information Act but is also not intentionally made public (see the definition of **public data**). Examples include salary information, employee name & title, meeting minutes, specific e-mail messages. (For a complete list, see The 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 widespread availability of such information will enable others to make creative contributions in pursuit of the University's mission.

- Networked Cameras that View University Assets and Public Spaces:
  Any camera (fixed or temporary), regardless of intended purpose, that has been determined to be in a location that can enhance public safety. This type of camera may include cameras that are integrated in an access control device (door station), emergency telephone, or installed for another purpose.

- 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:
In order to provide a safe and secure environment while respecting individual privacy rights in accordance with University standards and state and federal laws, the University has established a process for the installation of all networked cameras that view University assets and public spaces in University facilities and on University property; and the handling, viewing, retention, dissemination, and destruction of records in accordance with the regulations of the Virginia Public Records Act 42.1-76 et seq. of the Code of Virginia.

The existence of this policy does not imply or guarantee that cameras will be monitored in real time 24 hours a day, seven days a week.

1. **Authorization and Installation:**
   University department/schools, organizations, vendors and contractorŭs requests for authorization will include the proposed location of cameras that view University facilities or public spaces, justification of the proposed installation, and identification of funding source(s) for purchase and on-going maintenance of cameras. The University Police Department (UPD) and the department/school will execute a Memorandum of Understanding for all camera installations.

   University department/schools, organizations, vendors or contractors complete the Camera Installation Request Form and submit it to UPD requesting an assessment of the proposed installation. The Camera Installation Request Form will be reviewed by the Camera Oversight Group. The group will either approve or deny the request. Cameras in retail or other environments intended to primarily prevent theft or preserve assets or for purposes other than public safety may require an alternative funding source for installation.

   Upon approval by the Camera Oversight Group, UPD will coordinate with the department/school and oversee all activities associated with completing the request. Information Technology Services (ITS) will assist with securing and surveying network access.

   If the Camera Oversight Group 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 decide installation is critical to their operation. If this is the case, they may go forward with the following requirements:

   **The installation of "dummy" cameras that do not operate is prohibited.**

   Removal of cameras without authorization of UPD and the Camera Oversight Groups is prohibited.

   a. The camera must connect to the Universityŭs centralized video management system and must fulfill current University standards for the equipment and equipment maintenance.

   b. Purchase, installation, and maintenance shall be the sole responsibility of the department, school, program, or University organization.

   c. The department, school, program, University organization or University contractor will be required to maintain the camera in working order including funding any repairs or replacement necessary. All repairs or replacement shall be completed in a timely manner after notification that the camera is non-functioning or requires maintenance.

2. **Placement of Cameras:**
   Camera assessments will be completed by UPD to identify threats, security vulnerabilities, and other needs. Cameras will not normally be installed in areas where there is a reasonable expectation of privacy including, but not limited to: restrooms, private student resident hall rooms, medical patient rooms, and locker rooms.

   All public notifications that reference camera installation will be maintained and disseminated at the discretion of UPD.

3. **Access and Camera Monitoring:**
Not all University cameras are monitored continuously under normal operating conditions but may be monitored by UPD for legitimate safety and security purposes that include but are not limited to: monitoring restricted access areas/locations, monitoring traffic for special events, conducting criminal investigations, and enhancing response of public safety agencies such as police, fire, and emergency medical services.

   Access to live or recorded video from cameras shall be limited to authorized personnel approved by UPD who may include consultation with the Camera Oversight Group.

   The UPD Monitoring Station Supervisor or designee will review all requests, including those pre-approved, regarding the release or review of recorded video. Release or review of recorded video images will not occur without authorization by UPD. Release or withholding of such records shall be in accordance with the law, and when appropriate, consultation with University Counsel.

4. **Appropriate Use and Confidentiality:**

   a. Personnel are prohibited from using or disseminating information acquired from University cameras, except for official purposes. All information and observations made in the use of cameras are considered controlled data and can only be used for authorized University and law enforcement purposes, or as otherwise required by law. University Counsel will have access to the recordings as needed and/or requested.

      Sharing of user credentials and passwords for camera access is strictly prohibited.

   b. The camera system may not be used to unlawfully harass, intimidate, or discriminate against any individual or group.

   c. Camera recordings may not be used in the course of personnel policy infractions unless approved by the Vice President & Chief Human Resources Officer (or designee).

   d. The use of camera recordings for any purpose not detailed within this policy is subject to review by UPD who may consult with University Counsel.

5. **Training:**
UPD Camera Control Operators will receive regular training in the technological, legal, and ethical parameters of appropriate camera use.

   All other individuals that have been granted camera access shall receive a copy of this policy and provide written acknowledgement that they have read and understand its contents.

6. **Storage, Retention, Disposal of Recordings and Maintenance:**

   a. Storage, retention, and disposal of recordings will follow the regulations of the Virginia Public Records Act 42.1-76 et seq. of the Code of Virginia.

   b.

Recorded video will be stored for a period of no less than seven (7) days. When retained as part of a criminal investigation or court proceeding (criminal or civil), or other bona fide use as approved by the Chief of Police or designee and the University Records Officer, retention may be longer. (If additional storage time of recorded video is approved for other bona fide use, the department may be required to bear the cost the additional storage.)

7. **Exemptions:**
This policy does not apply to stand-alone cameras which are principally used for purposes other than safety and security functions such as video recording classroom lectures, athletic events, broadcasts or for post-game review; concerts; plays; or research experiments.

8. **Responsibilities:**

a. The ***Office of Safety and Emergency Preparedness (OSEP)*** is responsible for:

- Convening the Camera Oversight Group as necessary;
- On-going enterprise assessments and camera placements in conjunction with UPD;
- Improving security and access across Grounds; and
- Collaborating with department/schools to implement camera security recommendations.

b. The ***University Police Department*** is responsible for:

- Selecting, coordinating, operating, managing, and monitoring all University cameras pursuant to this policy;
- Assessing new camera locations in coordination with OSEP, ITS, the Office of the Architect, and Office of Facilities Management;
- Conducting an evaluation of existing camera locations as required/needed with OSEP; and
- Maintaining and testing of the video management system and, with OSEP, reviewing any complaints regarding the utilization of cameras and adherence to the policy. (Appeals of a decision made by the Chief of University Police will be made to and reviewed by the Executive Vice President & Chief Operating Officer.)

c. ***Information Technology Services*** is responsible for:

-

Assessing new camera locations in coordination with UPD and OSEP;

- Maintaining a separate virtual network for the video management system; and
- Enabling networking for camera locations as needed.

d. ***Office of the Architect*** is responsible for:

- Assessing new camera locations in coordination with UPD and OSEP; and
- Assisting in installation of cameras as needed.

e. ***Departments Using the Video Management System*** are responsible for:

- Implementing and complying with this policy; and
- Maintaining installed cameras in coordination with UPD and ITS, if applicable.

f. ***University Faculty and 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.

g. ***Office of Facilities Management*** is responsible for:

- Assessing new camera locations in coordination with UPD and OSEP;
- Assisting in installation of cameras as needed; and
- Facilitating compliance of this policy with subcontractors.

9. **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) will be subject to criminal prosecution and University action, as applicable.

Questions about this policy should be directed to the Contact Office(s).

Procedures:

1. Complete a Camera installation Request Form and submit to UPD requesting an assessment of the proposed installation.
2. A member of the Camera Oversight Group will be in contact regarding the request within ten (10) business days.

Related Information:
Student Standards of Conduct
Employee Standards of Conduct
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 Clinical Staff Code of Conduct
Medical Center HR Policy HR701 Employee Standards of Performance and Conduct
Major Category: Safety, Security and Environmental Quality
Next Scheduled Review: 07/13/2020
Approved by, Date: Policy Review Committee, 06/27/2017
Revision History: Revised 6/27/17, updated 5/6/2015. Supersedes (previous policy): XI.E.1, Use of Surveillance Cameras

**Source URL:** https://uvapolicy.virginia.edu/policy/SEC-034