Edit Policy

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

Date: 04/06/2015 Status: Final Last Revised: 09/11/2019

Policy Type: University
Contact Office: Safety & Security (Department of)
Oversight Executive: Executive Vice President and Chief Operating Officer

Applies To:
Academic Division and 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 in a way that enhances safety and security while respecting the privacy expectations of members of the University community.

Definition of Terms in Statement:

- Internal Use Data:
  Data that is typically a public record available to anyone in accordance with 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 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 `l regardless of whether it is a paper record, an electronic file, an audio or video recording or any other format `l that is prepared or owned by, or in the 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/or recording public areas for the purposes of enhancing safety and security of people and property, discouraging criminal activity, and investigating 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 camera requests and approvals, composed of representatives from these areas: Safety and Security (including the Director of Safety and 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.

- Private Areas:
  Areas including but not limited to: non-common areas of residence halls, residence hall corridors, 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 therapy or treatment are considered private areas.

- 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:
Prior to the purchase of any networked camera that will be installed in a University owned, leased, or operated facility to view public or private areas, regardless of cost, approval must be granted by the Networked Camera Oversight Group. The requirements for the installation and management of 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 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.

Exceptions:
This policy does not apply to:

1. Use of cameras solely for the purpose of:
    - remote monitoring of facility construction and progress;
    - videotaping of athletic events for post-game reviews;
    - carrying out human subject and animal research (which use is governed by University policies for research) or other legitimate educational purposes; and
    - 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; and
    - parking enforcement.

1. **Authority:**
   Oversight of 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:
    a. design, maintenance, and review of a University strategy for the procurement, deployment, and use of networked cameras, including this and related policies;
    b. design and approval of University standards for networked cameras and their use;
    c. creation of the standard University networked camera system or service;
    d. authorization of the placement of all networked cameras;
    e. authorization of the purchase of any new networked camera systems;
    f. review of existing networked camera systems and installations and identification of modifications required to bring them into compliance with this policy; and
    g. creation and approval of procedures for the use of networked cameras.
2. **Networked Camera Placement:**
    a. 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.
    b. All networked camera equipment must comply with University standards for the equipment and must be connected to the Universityŭs network.
    c. Departments and schools desiring the installation and use of networked cameras must submit a request for such installation to the Department of Safety and Security

via the on-line Networked Camera Installation Request Form.

d. All requests for networked cameras must include the location for the camera placement for the University facility or public space(s) and the identification of a funding source for the purchase and maintenance of the cameras.
e. A member of the Department of Safety and Security team 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 Camera Oversight Group to review the request.
f. The Networked Camera Oversight Group will review the request and either approve or deny the request.
g. Upon approval by the Networked Camera Oversight Group, the Department of Safety and Security coordinates with the department/school and oversees all activities associated with completing the request.
h. A Memorandum of Understanding (MOU) between the department/school and the Department of Safety and Security must be executed for all networked camera projects at the time the system is commissioned and turned over to the department/school for use.
i. Use of networked cameras is limited to public areas. Video surveillance must not be conducted in private areas owned or controlled by the University unless specifically authorized by the Chief of Police.
j. Networked cameras must not be directed at the windows of any privately-owned residence not located on University property. Pan Tilt Zoom (PTZ) cameras that can view windows of privately-owned residences must have the ability to ŏmaskǫ these windows by utilizing prohibitive software designed to prevent viewing.
k. 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.
l. Inoperative, placebo, or ŏdummyǫ 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.
m. If the Networked 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 appeal the decision to the Networked Camera Oversight Group.
n. Removal of cameras without authorization from the University Police Department (UPD) and the Networked Camera Oversight Group is prohibited.

3. **Camera Monitoring and Access to Recordings:**

a. ***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 response of public safety agencies such as police, fire, and emergency medical services.
b. ***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 in accordance with the law, and when appropriate, consultation with University Counsel.

4. **Appropriate Use and Confidentiality:**

a. Video monitoring for security purposes is conducted in a professional, ethical, and legal manner. Monitoring individuals based on characteristics of race, gender, sexual orientation, disability, or other protected classification is prohibited.
b. 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 internal use 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.
c. Sharing of user credentials and passwords for camera access is strictly prohibited.
d. Camera recordings must not be used in the course of personnel policy infractions unless approved by the Vice President & Chief Human Resources Officer (or designee).
e. 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:**

a. UPD Camera Control Operators must receive regular training in the technological, legal, and ethical parameters of appropriate camera use.
b. All other individuals that have been granted camera access must be given a copy of this policy and be provided the appropriate level of training necessary.

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

a. 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.
b. Recorded video is stored for a period of no less than fourteen (14) days. When retained as part of a criminal investigation or court proceeding, or other bonafide use as approved by the 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.

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 a Networked Camera Installation Request Form and submit to the Department of Safety and Security 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 ten (10) business days of receipt of the request.]

Related Information:
Employee Standards of Conduct
Disciplinary Suspension or Termination of Academic Faculty
HRM-050: Protection of Minors and Reporting Abuse
IRM-012: Privacy and Confidentiality of University Information

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: 09/11/2022
Approved by, Date: Policy Review Committee, 06/27/2017
Revision History: Revised 9/11/19; 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