Safety and Security Camera Acceptable Use Policy

No. 5617

Policy Effective Date:
3/1/2010

Last Revision Date:
3/14/2017

Policy Owner:
Sherwood Wilson

Policy Author:
(Contact Person)
Kayla Smith

Affected Parties:
Undergraduate
Graduate

1.0 Purpose

Virginia Tech is committed to enhancing the quality of life of the campus community by integrating the best practices of safety and security with technology. A critical component of a comprehensive security plan is the utilization of a security and safety camera system. The surveillance of public areas is intended to deter crime and assist in protecting the safety and property of the Virginia Tech community. This policy addresses the university's safety and security needs while respecting and preserving individual privacy.

To ensure the protection of individual privacy rights in accordance with the university's core values and state and federal laws, this policy is adopted to formalize procedures for the installation of surveillance equipment and the handling, viewing, retention, dissemination, and destruction of surveillance records. The purpose of this policy is to regulate the use of camera systems used to observe and record public areas for the purposes of safety and security. 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.

2.0 Policy

The Virginia Tech Police Department (VTPD) has the authority to select, coordinate, operate, manage, and monitor all campus security surveillance systems pursuant to this policy. All departments using camera surveillance are responsible for implementing and complying with this policy in their respective operations.

All existing uses of security camera systems will be required to comply with the policy at a future date. A notification of the compliance date will be made 12 months in advance. Unapproved or nonconforming devices will be removed prior to the compliance date.

A university Surveillance Oversight Committee (SOC) is an operational committee established by the Vice President for Administration to oversee implementation of this policy. Proposed policy revisions will be reviewed by the SOC and the University Safety and Security Policy Committee.

2.1 Responsibilities

VTPD, in conjunction with Information Technology and the Office of Emergency Management (OEM), is responsible for realization and assimilation of the policy.

Information Technology and the VTPD are responsible for advising departments on appropriate applications of surveillance technologies and for providing technical assistance to departments preparing proposals for the purchase and installation of security camera systems.

VTPD and Information Technology shall monitor developments in the law and in security industry practices and technology to ensure that camera surveillance is consistent with the best practices and complies with all federal and state laws.

VTPD and Information Technology will review proposals and recommendations for camera installations and review specific camera locations to determine that the perimeter of view of fixed location cameras conforms to this policy. Proposals for the installation of surveillance cameras shall be reviewed by the Chief of Police or designee. Recommendations shall be forwarded to the SOC.

VTPD and OEM will assess new camera locations and will conduct an evaluation of existing camera locations and incidents as necessary.

Maintenance and testing will be the responsibility of the department utilizing the camera system.

VTPD will review any complaints regarding the utilization of surveillance camera systems and determine whether this policy is being followed. Appeals of a decision made by the Chief of Police will be made to and reviewed by the SOC which will make a recommendation to the Vice President for Administration, who will render a decision. An appeal of the Vice President for Administration's decision may be taken to the university President who is the final arbiter.

2.1.1 Responsibilities of Surveillance Oversight Committee (SOC)

The SOC will be responsible for reviewing and approving or denying all proposals for security camera equipment recommended by the Chief of Police. The SOC shall be responsible for the review and approval of any requested exceptions to this policy. The SOC shall propose to the Vice President for Administration appropriate changes to this policy as needed.

The SOC shall be comprised of five members:

- The Chief of Police or designee, Chair of the SOC
- Chief Information Officer or designee
- Vice President for Student Affairs or designee
- Associate Vice President and Chief Facilities Officer or designee
- Assistant Vice President for Emergency Management or designee

2.1.2 Responsibilities for Review of External Requests for Records Release

The VTPD will review all external requests to release records obtained through security camera surveillance. The VTPD will seek consultation and advice from University Legal Counsel and other departments as deemed appropriate related to these requests prior to the release of any records.

2.2 Scope

This policy applies to all personnel, departments, and colleges of Virginia Tech in the use of security cameras and their video monitoring and recording systems. Security cameras may be installed in situations and places where the security and safety of either property or persons would be enhanced. Cameras will be limited to uses that do not violate the reasonable expectation of privacy as defined by law. Where appropriate, the cameras may be placed

campus-wide, inside and outside buildings. Although the physical cameras may be identical, the functions of these cameras fall into three main categories:

A. **Property Protection:** Where the main intent is to capture video and store it on a remote device so that if property is reported stolen or damaged, the video may show the perpetrator. Examples: an unstaffed computer lab, an unstaffed science lab, or a parking lot.

B. **Personal Safety:** Where the main intent is to capture video and store it on a remote device so that if a person is assaulted, the video may show the perpetrator. Examples: a public walkway, or a parking lot.

C. **Extended Responsibility:** Where the main intent is to have the live video stream in one area monitored by a staff member in close proximity. In this case video may or may not be recorded. Example: a computer lab with multiple rooms and only one staff.

2.3 General Principles

Information obtained from the cameras shall be used for safety and security purposes and for law and policy enforcement, including, where appropriate, student judicial functions. Information must be handled with an appropriate level of security to protect against unauthorized access, alteration, or disclosure in accordance with Policy 7105, Policy for Protecting University Information in Digital Form (http://www.policies.vt.edu/7105.pdf).

All appropriate measures must be taken to protect an individual's right to privacy and hold university information securely through its creation, storage, transmission, use, and deletion.

All camera installations are subject to federal and state laws.

Departments requesting security cameras will be required to follow the procedures outlined in this policy.

2.3.1 Placement of Cameras

The locations where cameras are installed may be restricted access sites such as a departmental computer lab; however, these locations are not places where a person has a reasonable expectation of privacy. Cameras will be located so that personal privacy is maximized.

No audio shall be recorded except in areas where no one is routinely permitted. Requests to utilize audio surveillance that does not comply with this requirement will be evaluated on a case by case basis by the SOC.

Camera positions and views of residential housing shall be limited. The view of a residential housing facility must not violate the standard of a reasonable expectation of privacy.

Unless the camera is being used for criminal investigations, monitoring by security cameras in the following locations is prohibited:

- Student dormitory rooms in the residence halls
- Bathrooms
- Locker rooms
- Offices
- Classrooms not used as a lab

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

Unless being used for criminal investigations, all video camera installations should be visible.

2.3.2 Access and Monitoring

All recording or monitoring of activities of individuals or groups by university security cameras will be conducted in a manner consistent with university policies, state and federal laws, and will not be based on the subjects' personal characteristics, including age, color, disability, gender, national origin, race, religion, sexual orientation, or other protected characteristics. Furthermore, all recording or monitoring will be conducted in a professional, ethical, and legal manner. All personnel with access to university security cameras should be trained in the effective, legal, and ethical use of monitoring equipment.

University security cameras are not monitored continuously under normal operating conditions but may be monitored for legitimate safety and security purposes that include, but are not limited to, the following: high risk areas, restricted access areas/locations, in response to an alarm, special events, and specific investigations authorized by the Chief of Police or designee.

For **Property Protection** and **Personal Safety** cameras, access to live video or recorded video from cameras shall be limited to authorized personnel of the department which installed the cameras, the Police Department and other persons authorized by the Chief of Police or designee. The copying, duplicating and/or retransmission of live or recorded video shall be limited to persons authorized by the Chief of Police or designee.

A record log will be kept of all instances of access to, and use of, recorded material. Nothing in this section is intended to limit the authority of the Virginia Tech Police Department (VTPD) in law enforcement activities.

2.3.3 Appropriate Use and Confidentiality

Personnel are prohibited from using or disseminating information acquired from university security cameras, except for official purposes. All information and/or observations made in the use of security cameras are considered confidential and can only be used for official university and law enforcement purposes. Personnel are expected to know and follow university Policy 7000, Acceptable Use and Administration of Computer and Communication Systems (http://www.policies.vt.edu/7000.pdf) and the Acceptable Use of Information Systems at Virginia Tech (http://www.vt.edu/about/acceptable-use).

2.3.4 Use of Cameras for Criminal Investigations

The use of mobile or hidden video equipment may be used in criminal investigations by the VTPD. Covert video equipment may also be used for non-criminal investigations of specific instances which may be a significant risk to public safety, security and property as authorized by the Chief of Police or designee.

2.3.5 Exceptions

This policy does not apply to cameras used for academic purposes. Cameras that are used for research would be governed by other policies involving human subjects and are, therefore, excluded from this policy.

This policy does not address the use of Webcams for general use by the university (e.g., on the official Virginia Tech website). This policy also does not apply to the use of video equipment for the recording of public performances or events, interviews, or other use for broadcast or educational purposes. Examples of such excluded activities would include videotaping of athletic events for post-game review, videotaping of concerts, plays, and lectures, or videotaped interviews of persons. Automated teller machines (ATMs), which may utilize cameras, are exempt from this policy.

3.0 Procedures

Departments requesting security cameras will be required to follow the procedures outlined in this policy.

3.1 Installation

Individual colleges, departments, programs, or campus organizations installing video surveillance equipment shall submit a written request to their appropriate dean or vice president describing the proposed location of surveillance devices, justifying the proposed installation, and identifying the funding source or sources for purchase and ongoing maintenance.

- The vice president, dean or designee will review the request and recommend it to the Chief of Police, if appropriate.
- The Chief of Police or designee will review all proposals from deans and vice presidents. Upon completion of review of the project, the Chief of Police will forward the proposal to the SOC with a recommendation.
- The SOC will be responsible for reviewing and approving or denying all proposals for security camera equipment recommended by the Chief of Police.

Network Infrastructure and Services (NI&S) shall oversee the installation of all approved security camera systems with the assistance of the VTPD, the Division of Information Technology, and Facilities, as required.

Purchasing (HokieMart) will not accept, approve, or process any order for security camera systems without the approval of the SOC.

3.2 Training

Camera control operators shall be trained in the technical, legal, and ethical parameters of appropriate camera use.

Camera control operators shall receive a copy of this policy and provide written acknowledgement that they have read and understood its contents.

3.3 Operation

Video surveillance will be conducted in a manner consistent with all existing university policies.

Camera control operators shall monitor based on suspicious behavior, not individual characteristics.

Camera control operators shall **not** view private rooms or areas through windows.

All operators and supervisors involved in video surveillance will perform their duties in accordance with this policy.

3.4 Storage and Retention of Recordings

No attempt shall be made to alter any part of any surveillance recording. Surveillance centers and monitors will be configured to prevent camera operators from tampering with or duplicating recorded information.

Surveillance records shall not be stored by individual departments. All surveillance records shall be stored in a secure university centralized location for a period of 15 days and will then promptly be erased or written over, unless retained as part of a criminal investigation or court proceedings (criminal or civil), or other bona fide use as approved by the Chief of Police or designee. Individual departments shall not store video surveillance recordings.

A log shall be maintained of all instances of access to or use of surveillance records. The log shall include the date and identification of the person or persons to whom access was granted.

4.0 Definitions

5.0 References

University Policy 7000, Acceptable Use and Administration of Computer and Communication Systems
http://www.policies.vt.edu/7000.pdf

University Policy 7105, Policy for Protecting University Information in Digital Form
http://www.policies.vt.edu/7105.pdf

6.0 Approval and Revisions

Approved March 1, 2010 by Vice President for Administrative Services, Sherwood G. Wilson.

- Revision 1
  - Section 2 – addition of wording “by January 2013” and deletion of “within 12 months of the approval of this policy.”
  - Section 2.3.1 – change “surveillance” to “investigations.”
  - Technical corrections, updates and insertion of hyperlinks.

  Approved March 14, 2011 by Vice President for Administrative Services, Sherwood G. Wilson.

- Revision 2
  - Section 2 – removal of “shall be brought into compliance with this policy January 2013” and addition of “will be required to comply with the policy at a future date. A notification of the compliance date will be made 12 months in advance.”
  - Section 2.3 – added “safety and security purposes” to the list of purposes for camera use
  - Section 2.3.2 – modified list of individuals who may access live or recorded video for personal protection and personal safety cameras, and added “The copying, duplicating and/or retransmission of live or recorded video shall be limited to persons authorized by the Chief of Police or designee.”

- Section 3.1 – removed requirement to provide cost estimate
- Section 3.4 – changed 30 day storage period to 15 days
- Technical corrections to titles of individuals and departments
- Added option for individuals to appoint a designee for specific responsibilities

Approved April 17, 2012 by the University Safety and Security Policy Committee.

Approved April 17, 2012 by President Charles W. Steger upon recommendation of the University Safety and Security Policy Committee.

- Revision 3
  - Updated membership of the SOC by removing representative from Business Services, due to change in responsibilities.
  - Updated titles and department names.

Approved March 14, 2017 by the University Safety and Security Policy Committee.

Approved March 14, 2017 by President Timothy D. Sands upon recommendation of the University Safety and Security Policy Committee.