UNIVERSITY OF TENNESSEE, KNOXVILLE
CAMPUS PROCEDURE ON THE ACCEPTABLE USE OF VIDEO SURVEILLANCE

1. Purpose

The University of Tennessee, Knoxville is committed to enhancing the quality of life of the campus community by integrating the best practices of safety and security with technology. The purpose of this procedure is to provide guidelines for the use of security cameras on property owned and/or utilized by the University of Tennessee, Knoxville in a way that enhances security and aids law enforcement while respecting the privacy rights of members of the University community in accordance with the university's core values and state and federal laws. This procedure formalizes procedures for the installation of video surveillance equipment and the handling, viewing, retention, dissemination, and destruction of video surveillance records. The existence of this procedure does not imply or guarantee that video surveillance equipment will be monitored in real time 24 hours a day, seven days a week. The University of Tennessee assumes no additional liability for campus safety as a result of utilizing video surveillance systems and/or making determinations of when it is/is not monitored in real time.

2. Scope

This procedure applies to all employees and units of the University of Tennessee, Knoxville in the use of video surveillance equipment on property owned or controlled by the University. All units using video surveillance equipment are responsible for implementing and complying with this procedure in their respective operations.

Video surveillance equipment may be installed in places where the security and safety of either property or persons would be enhanced by the installation of such equipment, including the interior and exterior of facilities. Video surveillance equipment will be limited to uses that do not violate an individual's reasonable expectation of privacy as defined by law. The functions of video surveillance equipment fall into four 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 a live video stream in one area monitored by a staff member in close proximity to the area. In this case video may or may not be recorded. Example: a computer lab with multiple rooms and only one staff.

D. **Investigation of Criminal Activity:** The ability for law enforcement to review recorded or live video footage in relation to a criminal act. Example: Theft of a computer from a building or department.

This procedure shall not apply to use of cameras for reasons unrelated to surveillance activity, including:

- Remote monitoring of facilities construction and progress
- Instructional, academic, athletic or artistic purposes
- Research that is governed by other policies involving human subjects or animals
- In health treatment settings governed by the Health Insurance Portability and Accountability Act (HIPAA)
- Monitoring automated teller machines (ATMs)
- To conduct business or video conferences
- To conduct an audit of law enforcement investigation
- In accordance with a court order

Nor shall this procedure apply to cameras used by law enforcement in the following manners:

- Covert operations for the purpose of criminal surveillance
- Mobile cameras used in, on, or about law enforcement
- Body-worn or otherwise portable cameras used during the course of investigations

3. Responsibilities

- The University of Tennessee Police Department (UTPD), in conjunction with the Department of Physical Security (DPS)~~,~~ is responsible for implementation of this procedure. UTPD has the authority to select, coordinate, operate, manage, and monitor all campus video surveillance equipment pursuant to this procedure.

- The Department of Physical Security is responsible under the authority of the Associate Vice Chancellor of Public Safety to oversee implementation and revisions of this procedure.

- UTPD, DPS and OIT are responsible for advising units on appropriate applications of video surveillance equipment and for providing technical assistance to units preparing proposals for the purchase and installation of video surveillance equipment.

- UTPD, DPS and OIT shall monitor developments in the law and in security industry practices and technology to ensure that the university's use of video surveillance equipment is consistent with the security industry's best practices and complies with all federal and state laws.

- UTPD, DPS and OIT will review departmental proposals for video surveillance equipment installations and review specific locations of video surveillance equipment to determine that the perimeter of view of fixed location video surveillance equipment conforms to this procedure. Proposals for the installation of video surveillance equipment shall be reviewed by the Director of Physical Security or designee. DPS will be responsible for reviewing, approving or denying all proposals for video surveillance

equipment planned or designed.

- The Director of Physical Security, or his/her designee, will review any complaints regarding the utilization of video surveillance equipment and determine whether this procedure is being followed. Appeals of a decision made by the Director of Physical Security, or his/her designee, will be made to and reviewed by UTPD and DPS. A department can appeal the decision of by requesting an appeal to the Director of Physical Security or his official designee with the option of a final appeal to the Associate Vice Chancellor of Public Safety.
- DPS will maintain an inventory of video surveillance equipment installed pursuant to this procedure.
- DPS shall propose revisions to this procedure to the Associate Vice Chancellor of Public Safety.

4. General Principles

4.1 Security Camera Placement

The locations where video surveillance equipment are installed may be restricted access sites such as a departmental computer lab; if these locations are not places where a person has a reasonable expectation of privacy. Video surveillance equipment will be located in areas considered public access areas.

Camera positions and views of residential building units shall be limited. The view of a residential housing facility shall not be greater than what is afforded by unaided, human vision. Viewing through the windows of private rooms is prohibited.

Unless the video surveillance equipment is being used for criminal investigations in accordance with law, monitoring by video surveillance equipment in the following locations is prohibited:

- Student dormitory rooms in the residence halls
- Bathrooms
- Single Occupancy Offices
- Locker rooms
- Health treatment rooms

The installation of "dummy" video surveillance equipment (i.e., equipment that does not operate) is prohibited.

4.2 Access and Monitoring

All recording or monitoring by video surveillance equipment shall 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, or

sexual orientation. Furthermore, all recording or monitoring will be conducted in a professional and legal manner.

There is no expectation for video surveillance equipment to be monitored live under normal operating conditions but may be monitored live for legitimate safety and security purposes if approved by the Director of Physical Security or designee (e.g., high risk areas, restricted access areas/locations, in response to an alarm, special events, specific investigations).

Access to live video or recorded video from video surveillance equipment shall be limited to persons authorized by the Director of Physical Security or designee. When an incident is reported, the department or unit head responsible for the area in question may request Director of Physical Security to review video surveillance records relating to an incident. As circumstances require, the Director of Physical Security can authorize others to review video surveillance records. Authorization occurs with confirmation for the Associate Vice Chancellor of Public Safety. The video management system operating platform has a built in user access log to identify what activity has taken place for reference purposes. Nothing in this section is intended to limit the authority of UTPD in law enforcement activities

4.3 Appropriate Use and Confidentiality

Access to the video surveillance system and rights therein, shall be limited to the minimum required to perform the functions of an individual's position. Departments interested in viewing and monitoring the live views of their cameras need to complete a camera access request form.

Video surveillance records are considered confidential and can only be used for official university and law enforcement purposes upon the approval of the Director of Physical Security, or designee. Video surveillance records shall be handled with an appropriate level of security to protect against unauthorized access, alteration, or disclosure and in accordance with University of Tennessee System Procedure IT 110, Acceptable Use of Information Technology Resources.

University of Tennessee System Procedure IT 110, Acceptable Use of Information Technology Resources
https://universitytennessee.proceduretech.com/docview/?docid=157&public=true.

4.4 Storage and Retention of Recordings

No attempt shall be made to alter any part of any video surveillance recording. VMS servers will be audited to monitor any exporting of video surveillance records.

All video surveillance records shall be stored in a secure university centralized location for a period of no less than 14 days and will then promptly be erased or written over as storage limits are exceeded, unless retained as part of a criminal investigation or court proceedings (criminal or civil), as part of another bona fide use as approved by DPS, or in response to a preservation request issued by the Office of the General Counsel.

Any unit requesting rights to export video surveillance records must develop a written procedure. This procedure should include what personnel will process the exports, where the exported records will be stored, storage retention periods, the process for eliminating records past retention, and anyone these records might be shared with. The Director of Physical Security, or his/her designee, must approve this procedure before export rights will be granted.

Any unit in violation of this procedure may result in the loss of individual or unit access to the video surveillance system.

4.5 Equipment Standards

The type of video surveillance equipment and operating platform is Avigilon. All information pertaining to specific products (cameras, video recorders, etc.) can be viewed at www.avigilon.com. Any approved equipment purchase exceeding $5,000 shall follow Fiscal Procedure FI0410. Exceptions to the specified equipment standard shall be reviewed and approved by DPS. All purchases should conform to the Enterprise licensing version of Avigilon.

4.6 Video Surveillance Cost

All exterior doors, critical facilities (i.e. electrical, mechanical), and IT spaces (i.e. data rooms, data centers) will be provided by the university as part of basic video surveillance best practices.

A requestor must fund any cameras beyond the campus standards. This applies to purchase, installation, maintenance, and storage fees.

5. Procedures

5.1 Installation

Units seeking approval for installation of video surveillance equipment shall submit a written request through their appropriate dean or vice chancellor describing the proposed location of the video surveillance equipment, justifying the proposed installation, and identifying the funding source or sources for purchase and ongoing maintenance.

University of Tennessee Knoxville Camera Request Form
https://safety.utk.edu/police/wp-content/uploads/sites/2/2021/04/Camera-Request-FormUTK-revision-2.pdf

The Director of Physical Security, or designee will review all proposals submitted regarding video surveillance. Upon completion of review of the project, DPS will approve or deny the project for completion.

OIT Communications shall oversee the installation of all approved video surveillance equipment with the assistance of the DPS, OIT, and Facilities, as required.

5.4 Training

Video surveillance equipment control operators shall be trained in the requirements of this procedure and the technical, legal, and ethical parameters of appropriate video surveillance equipment use. Training will be provided by DPS personnel or online tutorials offered by the manufacturer. Authorized departmental users as requested should provide confirmation of adherence to this procedure.

Video surveillance equipment control operators shall receive a copy of the Acceptable Use Procedure and provide written acknowledgement that they have read and understood its contents.

5.5 Operation

Video surveillance will be conducted in a manner consistent with this procedure and all other university policies.

Video surveillance equipment control operators shall monitor based on suspicious behavior, not individual characteristics.

The video management system operating platform has a built in user access log to identify what activity has taken place for reference purposes.

5.6 Surveillance Record Dissemination

Video surveillance records shall not be disseminated by individual units without following a written approved process. This is not limited to sharing exported video, but includes activities such as sharing screenshots or sharing your screen with an unauthorized person.

The Office of Communications & Marketing will process all external requests to release copies of video surveillance records in consultation with the Office of the General Counsel. Certain video surveillance records are confidential and protected from release under the Tennessee Public Records Act, Tennessee Code Annotated § 10- 7-504(m). In addition, certain video surveillance records may be exempt from mandatory disclosure under the Freedom of Information Act. See 5 U.S.C. 522, 41 C.F.R. Part 105-60.

DPS will process all internal requests for access to video in consultation with the Office of the General Counsel. Certain video surveillance records are confidential and protected from release under the Tennessee Public Records Act, Tennessee Code Annotated § 10- 7-504(m). In addition, certain video surveillance records may be exempt from mandatory disclosure under the Freedom of Information Act. See 5 U.S.C. 522, 41 C.F.R. Part 105-60.

6 Definitions

"Unit": Any administrative, academic, or research unit of the University of Tennessee, Knoxville.

"Video surveillance equipment": devices used to observe and record a single image (still, snapshot, photograph), a number of single images per time period (stop action, time laps), or multiple images (motion, video) for the purpose of surveillance. This term does not include cell phone cameras or University webcams.

7 References

University of Tennessee System Procedure IT 110, Acceptable Use of Information Technology Resources
https://universitytennessee.proceduretech.com/docview/?docid=157&public=true.

University of Tennessee Procedure IT0115, Information and Computer System Classification
https://universitytennessee.proceduretech.com/docview/?docid=158&public=true.

Request for Security Camera Access Form
https://safety.utk.edu/police/wp-content/uploads/sites/2/2021/10/Camera-Access-Request-Physical-Security.pdf