

# Security Surveillance Camera Guidelines

## I. OVERVIEW

The University of Oklahoma ("University") seeks to provide its respective communities with a safe and secure environment. When successfully deployed, security surveillance camera systems enhance overall campus safety and security, deter crime, and otherwise support the protection of people and property. A *security surveillance camera* is defined as information technology used for monitoring people's activities and response equipment that records people's activities in order to detect, deter, prevent, or investigate crime or other threats to public safety (such as terrorism).

The University recognizes that necessary steps must be taken to protect personal privacy and civil liberties when the University operates a security surveillance camera. As such, no security surveillance camera shall be installed or operated in any University campus location in which there is a reasonable expectation of privacy. Also, such installations or operations must not impinge on or unduly constrain the academic freedom or civil liberties of community members or their freedom of assembly and expression.

## II. PURPOSE

The purpose of these guidelines is to regulate the appropriate uses of security surveillance cameras on any University campus, including the retention and release of recorded images. These guidelines apply to cameras installed or activated specifically for purposes of enhancing campus safety and security, irrespective of the specific camera technology or whether the cameras are monitored in real time.

Recorded images from the security surveillance cameras are protected from disclosure to the public under the Oklahoma Open Records Act as information technology (under 51 O.S. §24A.28(A)(5)) and/or law enforcement records (under 51 O.S. §24A.8(B)). Recorded images may also be considered sensitive information whose confidentiality, integrity, and availability should be protected under any other applicable federal or state law, including Export Control laws, the Health Insurance Portability and Accountability Act ("HIPAA") and the Family Educational Rights and Privacy Act ("FERPA").

## III. SCOPE AND EXCLUSIONS

### A. Application of Guidelines

These guidelines apply to all University security surveillance cameras in existence on campus as of the effective date and any that are installed or modified thereafter.

These guidelines do not apply to security cameras located in the following areas:

- Clinical patient care areas
- Animal research areas

- Human subject research areas
- University tenants' camera systems, including but not limited to ATMs
- Camera systems used on any University owned or leased property that is not geographically contiguous with the University campuses in Norman, Oklahoma City, and Tulsa
- Video and audio systems used for law enforcement purposes, including but not limited to University police dashboard cameras installed in University-owned law enforcement vehicles and body cameras worn by University law enforcement personnel
- Video cameras that are used for non-security purposes, including video communication equipment used for video conferencing and classroom video equipment used for learning, instruction, and presentations
- Camera systems owned by third parties located in University owned or leased areas

#### B. Security Surveillance Camera Locations and Limitations

Except as provided above, efforts to promote campus safety and security by the use of security surveillance cameras are primarily focused on, but not limited to, protection of individuals including students, faculty, staff, and visitors and monitoring of:

- Any University owned, leased, and/or operated property and buildings that are geographically contiguous with the University campuses in Norman, Oklahoma City, and Tulsa;
- Rooms and labs containing high value equipment or information;
- Cash-handling areas where money is exchanged, such as University-owned ATMs and cashier locations; and
- Common areas and areas accessible to the public.

Security surveillance cameras generally may not be installed in areas where there is a reasonable expectation of privacy. These areas include, but are not limited to:

- Restrooms
- Locker rooms
- Occupied student residential rooms

Similarly, security cameras generally may not be installed where physical, visual, and/or electronic access controls are required by law or contract (e.g., where export-controlled technical data or equipment is present).

Security camera systems should not enable audio recording.

#### IV. OPERATOR ROLES AND RESPONSIBILITIES

Campus law enforcement will strictly control access to security surveillance cameras systems and recorded images in accordance with this Section VI of the Guidelines. The authorized users or operators of security surveillance cameras systems are campus law enforcement members or other staff members who have been assigned responsibility by the campus Chief of Police or a

designated representative ("Security System Operators").

Security System Operators must be trained and supervised by campus law enforcement in the responsible and effective use of these systems and technology, including the technical, legal, and ethical parameters of such use. Security System Operators will receive campus security training from campus law enforcement to help ensure compliance with relevant provisions of the Federal Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act and other applicable laws, policies, and guidelines.

Anyone who accesses, uses, manipulates, destroys, alters, or damages University information resources, recorded images, or property without authorization may be guilty of violating state or federal law, infringing upon the privacy of others, and/or threatening the integrity of information kept within these systems.

Security System Operators must sign an Agreement to Comply with the Security Surveillance Camera Guidelines (Attachment A) prior to operating any security surveillance camera system. Signed Agreements to Comply will be kept on file with campus law enforcement or their designee.

University departments and/or Human Resources must immediately notify campus law enforcement when the employment of any Security System Operator terminates.

**V. AUTHORIZATION AND APPROVAL OF EXISTING, NEW, AND MODIFIED SECURITY SURVEILLANCE CAMERAS**

All existing, new, and modified security surveillance cameras must comply with the terms and conditions of these Guidelines and must have final approval from the campus Chief of Police or a designated representative and the Department of Information Technology. IT shall review the camera system to determine whether the technology is appropriate and compatible with University systems. Campus law enforcement shall conduct a security review and advise on camera placement.

**VI. RECORDED IMAGES RETENTION, ACCESS, AND RELEASE**

Campus law enforcement is responsible for appropriately protecting information that may have been captured by cameras under its control. All recorded images generated by University security surveillance cameras must be stored in a secure location established by campus law enforcement and the Department of Information Technology, unless otherwise approved by campus law enforcement. All recorded images should be accessible by Security System Operators only as approved by campus law enforcement and configured to prevent unauthorized modification, duplication, or destruction. Requests by University departments or employees to review other University department recorded images for official University business must be made to campus law enforcement and shall follow the Guidelines for Requesting Recorded Images from Security Surveillance Cameras (Attachment B). These requests shall be made using the Recorded Images Request Form (Attachment C).

Recorded images should be retained for no more than twenty (20) calendar days unless there is a demonstrated business need, grantor requirement, or legal requirement, or unless the images are part of an ongoing criminal or civil court proceeding, employment investigation, legal hold, court order, or police case file. Extended retention time must be authorized in writing by the campus Chief of Police or the Office of Legal Counsel or their designated representatives.

Requests for access to or release of recorded images by individuals or entities outside of the University and/or for purposes other than official University business (such as an Open Records or Freedom of Information Act request) must be forwarded to the Open Records Office, which will review the request and make the final determination. Only the Open Records Office may make such determinations.

Recorded images may be shared by campus law enforcement with other law enforcement agencies as necessary, in accordance with applicable law and University policies.

## **VII. OVERSIGHT AND GOVERNANCE**

The campus Chief of Police, the General Counsel, and Vice Presidents for Administration and Finance, or their designated representatives shall convene as necessary in order to:

- Review and revise these Guidelines and related standards and procedures, and
- Review and approve major amendments to these Guidelines.

The campus Chief of Police, or his or her designee, or the Department of Information Technology, will:

- Maintain an up-to-date comprehensive inventory of permanent camera installations and image storage locations to facilitate the University's access to recorded images of possible crimes or incidents that require investigation; and
- Provide periodic administrative updates and guidance to security surveillance cameras systems operators.

## **VIII. VIOLATIONS AND SANCTIONS**

Alleged violations of these Guidelines will be reviewed and investigated by the campus Chief of Police or his/her designee, in consultation with the Office of Legal Counsel.

## **IX. EXCEPTIONS**

The campus Chief of Police, in consultation with the General Counsel and Vice Presidents for Administration and Finance or their designated representatives, may grant exceptions to these Guidelines, which may include but are not limited to situations where exceptions are necessary due to contractual requirements. Exceptions, with rationale, should be documented in writing and included in the inventory specified in Section VII.

**Attachment A**

**Agreement to Comply with the Security Surveillance Camera Guidelines**

The purpose of this form is to indicate agreement to follow the "Security Surveillance Camera Guidelines" ("Guidelines"), which were created to regulate the appropriate uses of security surveillance cameras on any University of Oklahoma ("University") campus, including the retention and release of recorded images. The Guidelines apply to cameras installed or activated, permanently or on a temporary basis, specifically for purposes of enhancing campus safety and security, irrespective of the specific camera technology or whether the cameras are monitored in real time.

**The Undersigned has read and understands the Guidelines and agrees to comply with the protocols listed therein in regards to the operation and carrying out of the Undersigned's duties at the University.**

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Position

## Attachment B

### Internal Guidelines for Requesting Recorded Images from Security Surveillance Camera

#### For Internal University Use Only

The recorded images from the University's security surveillance cameras are owned by the University. Campus law enforcement maintains control of and access to these recorded images. Other University departments and staff members may request these recorded images from campus law enforcement as provided by these Internal Guidelines ("Internal Guidelines"). The purpose of these Internal Guidelines is to describe "best practices" for requesting and distributing recorded images.

To request recorded images, the following steps should normally be followed:

- A. Request Record. Applicant shall submit a completed Recorded Image Request Form (Attachment C) for each recorded image request. This form shall be provided to campus law enforcement and shall require the following information:
  1. the name, title, and contact information of the person making the request for the recorded images;
  2. the description of recording requested, including date(s), time(s), and location(s); and
  3. the reason for request or other relevant information, which must further official University purposes.
- B. Review. Campus law enforcement shall review the request and consult with other University officials as may be necessary.
- C. Authorization. After reviewing the Recorded Image Request Form, campus law enforcement may: (i) authorize the request; (ii) deny the request; (iii) modify the request; or (iv) request additional information from the Applicant.
- D. Distribution. Upon campus law enforcement approval of a Recorded Image Request, the campus law enforcement will work with Applicant to provide recorded images in the appropriate format.
- E. Completion of Purpose:  
Upon completion of the Recorded Image Requested, the person who made the request shall properly destroy said Recorded Image Requested and confirm the destruction of the Recorded Image Requested to the appropriate Campus law enforcement agency.

**Attachment C**

Recorded Image Request Form For Internal University Use

Date of Request: \_\_\_\_\_

Applicant Name and Title and Department/College Information:

\_\_\_\_\_

Applicant Contact Phone Number and Email: \_\_\_\_\_

Supervisor Name and Signature: \_\_\_\_\_

Recorded Image Requested: \_\_\_\_\_

Time of Recording: \_\_\_\_\_

Date of Recording: \_\_\_\_\_

Location of Recording: \_\_\_\_\_

\_\_\_\_\_

Reason for Request:

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Other:

\_\_\_\_\_

\_\_\_\_\_

By executing this form, I understand that I may not share the Recorded Image Requested without proper permission from both my supervisor and the appropriate Campus law enforcement agency. I also agree upon completion of use of the Recorded Image Requested, I shall properly destroy the Recorded Image Requested and confirm the destruction of the Record Image Requested to the appropriate Campus law enforcement agency.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

FOR INTERNAL USE ONLY

Authorized

Denied \_\_\_\_\_

Modified \_\_\_\_\_

Name: \_\_\_\_\_

Need additional Information: \_\_\_\_\_