



Surveillance Camera Policy

Number:

Date: June 24, 2014

Department(s): Police Services, Information Technology

General Statement

1.1 The University of Central Oklahoma is committed to the management of surveillance video recordings and closed circuit television (CCTV) systems so that safety and security is enhanced while respecting the privacy rights of the university community and the general public.

Purpose and Principles

2.1 The purpose of this policy is to regulate the installation, use and overall management of surveillance camera systems used to record public areas of the campus for the purposes of safety and security. The presence of surveillance cameras is intended to achieve the following purposes:

- Helping to ensure safety of students, faculty, staff and visitors
- Deterring and controlling theft
- Deterring the potential for vandalism and the defacement of property
- Assisting in the identification of disruptive or threatening individuals
- Assisting in the resolution of crimes

2.1.1 To ensure proper implementation of camera systems on campus, this policy provides guidance for the design, installation, maintenance, management and use of systems and their recordings to ensure privacy and compliance with applicable policy and law.

2.1.2 This policy requires that all surveillance camera installations and their associated recording systems be linked to the University's approved central video management system and be observable (both live and recordings) and controllable by UCO Police and other authorized system users.

- Individuals, departments or other operating units are specifically prohibited from installing or operating cameras or other forms of image capturing devices including but not limited to webcams, stand-alone cameras, camcorders, etc. in any location on campus except as noted in this policy.
- Individuals encountering problems in offices or specific areas should report this information to UCO Police Services. Individuals may not utilize a webcam installed in a computer for surveillance purposes without approval and in coordination with UCO Police Services.

2.2 Information obtained from the cameras and their recordings shall be used exclusively for law and/or policy enforcement.

2.2.1 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. It is for this reason that surveillance cameras installed in all public areas/spaces need prior approval from UCO Police Services.

2.2.2 All departments/divisions and individuals requesting installation of camera systems or use of another department/divisions recordings or live images are required to follow this policy inclusive of its procedures (see Video Surveillance Procedure).

Scope

3.1 This policy applies to all staff, faculty, students, other academic personnel, contractors, vendors and visitors in facilities owned or controlled by the University of Central Oklahoma. It is intended only for use of closed circuit television (CCTV) systems installed and managed for the purposes outlined in 2.1 above. It does not apply to:

- Use of video recording and/or camera systems for any academic purpose.
- Use of video recording and/or camera systems related to any athletic purpose.
- Use of video recording and/or camera systems related to any promotional, fundraising or other non-security and safety purposes such as those performed by University Relations or other departments/divisions on campus.
- Use of video recording and CCTV technology for video conferencing.
- Use of fixed, mobile or portable video/audio recording systems utilized by UCO Police in the performance of their normal duties (e.g. dash cameras). UCO Police must comply with separate operational directives for use of these systems.
- "Web" cameras installed in desktop or portable computing devices in offices, labs, classrooms or other designated work or academic spaces unless the use of that camera is for a law enforcement or policy enforcement purpose.
- Use of recordings made by individuals using camera-based or other privately-owned video camera equipment for personal purposes while on campus owned or controlled property.

Responsibilities

4.1 UCO Police and Information Technology are responsible for realization and assimilation of this policy. These departments 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.

4.1.1 UCO Police and Information Technology will work with a vendor or vendors as needed in regard to design, installation, maintenance and overall management of surveillance camera systems on campus or in facilities controlled by the university (see Video Surveillance Procedure).

4.1.2 UCO Police and Information Technology shall seek and maintain awareness of best practices and technological changes to ensure that camera surveillance systems installed and maintained by UCO are appropriate, effective, efficient and compliant with applicable laws.

4.1.3 UCO Police and Information Technology will work with departments/divisions to review proposals and recommendations for surveillance camera system installations to ensure that camera placement and management of recordings are consistent with this policy to ensure privacy of individuals (see Video Surveillance Procedure).

4.1.4 Information Technology is responsible for maintaining the network components necessary for the proper and reliable use of cameras and recordings. This shall include cabling, switches, fiber optic lines, servers and software associated with surveillance camera systems on campus.

4.1.5 UCO Police will work with other departments/divisions to review any complaints from students, faculty, staff, vendors, contractors and visitors regarding the installation and use of surveillance cameras and recordings to ensure they comply with this policy.

4.2 Departments and divisions desiring installation and implementation of a surveillance camera system in their area are responsible for providing funding for the installation and long-term implementation of systems inclusive of cameras, mounting equipment, cables/wiring, vendor labor costs, video storage, software (inclusive of updates as may be appropriate), licensing fees, infrastructure upgrades, etc.

- The university recognizes that a significant cost factor in the management of a surveillance camera system is storage capacity of recordings. This policy requires that departments/divisions provide funding to ensure that recordings of all cameras allow for not less than ten (10) days of routine archiving for each installed camera at their intended resolution and operational settings. Departments, at their discretion and funding ability can extend the length of routine archiving or seek solutions to move recordings to alternate storage media within the limits of this policy.
- Per this policy, all data from surveillance camera systems on campus must be stored on site using the IT maintained infrastructure. Vendor-hosted solutions will be permitted in only limited circumstances such as remote site system installations.
- A portion of funding paid by the client department/division equivalent to current cost for hardware for data storage and necessary IT infrastructure (switches, cabling, etc.) will be placed in the IT Surveillance Camera budget during the purchasing phase of the project to acquire and maintain adequate data storage and connectivity. An reasonable annual fee per camera may also be charged based on need to maintain systems, etc. (see Surveillance Camera Procedure).

4.3 UCO Legal Services will review all media and public requests submitted to UCO Police Services to release records obtained through security camera surveillance systems in accordance to the Oklahoma Open Records Act, other applicable laws and university policy. Pursuant to law, UCO Police or other law

enforcement agencies with jurisdiction may request, in the case of an active criminal investigation, that release of recordings be denied unless a subpoena from a court of competent jurisdiction is presented to the university for their release.

- This policy will not restrict UCO from releasing images or information obtained from surveillance camera systems to aid in public appeals to help identify individuals and solve crimes that have occurred.

4.4 It is the responsibility of all departments and individuals with authorized access to camera operations and recordings to ensure that they are operated in a manner that is consistent with this policy and applicable laws.

- No person may take any action or fail to take action that improperly impacts privacy of individuals or integrity of the systems. This includes any improper release of recordings or allowing any unauthorized person to view, access or possess live or recorded images from any surveillance camera owned or controlled by the university. This policy also applies to corporate vendors used in the installation or maintenance of surveillance camera systems.
- No person may copy or distribute video recordings or still images unless authorized to do so. This includes authorized employees posting recordings/images to public media sites or otherwise sharing images with others. Recordings and images can only be used for official law enforcement and policy purposes.

4.5 No department, division or individual employee may seek to bypass the surveillance camera approval process (see UCO Video Surveillance Procedure) under any circumstance.

Placement of Cameras

5.1 Cameras or other image capturing systems installed by individual community members or departments without approval are prohibited in part because camera placement may jeopardize individual rights and violate state and federal law. UCO will work with the selected vendor to design individual installations that achieve lawful and desired outcomes. The locations where camera installations are not permitted include:

- Restrooms
- Dressing/locker rooms in athletic or artistic performance facilities.
- Individual faculty or staff offices or designated work spaces such as cubicles or shared work spaces.
- Conference or meeting rooms except for those installed for academic or video-conferencing purposes.
- Classrooms
- Student residence hall rooms or hallways in residence halls where group restrooms are accessed via a hallway.
- Any other location not permitted by law or university or regents policy.

5.2 Temporary installations of cameras requested through UCO Police Services for purposes of criminal investigation may be permitted in restricted areas pursuant to a valid court order and/or with the permission of the President (or his/her designate).

Signage

6.1 Any building, parking area or other location that has surveillance cameras installed on or in the building is required to have a sign placed at each public entrance that conveys the presence of video recording devices inside the structure. This notice will be conveyed through a simple sticker placed on the surface of public entrances (one per entrance minimum) or parking lot signage in a conspicuous location. The design of this notice is the responsibility of University Relations. The placement and maintenance is the responsibility of the Physical Plant. These stickers will be paid for and maintenance coordinated by UCO Police.

6.2 By this policy, at any location where there is audio and video recording, a separate sign or notice is required indicating that both audio and video recordings are occurring in that specific location.

Additional Policy Information

7.1 All surveillance camera systems and any individual components, additions, deletions or other changes to or initial installations must be designed in partnership with the approved corporate vendor and approved by Information Technology and Police Services before a purchase order can be issued pursuant to the UCO Video Surveillance Procedure.

7.2 All components related to a surveillance camera solution for any location on campus or in locations controlled by the university must use UCO **Surveillance Camera** systems for storage of recorded images (data) and must use networking cabling and equipment that are part of the UCO infrastructure. Prior approval (see Video Surveillance Procedure) is required in every case.

7.3 Placement of cameras, mounting equipment, cabling and other components necessary for the proper installation of surveillance camera systems cannot violate building codes or otherwise create a hazard such as breaching of a fire wall without proper fire blocking. Architectural and Engineering Services, UCO Code Compliance and other offices/departments, as may be appropriate, will be included in the planning phase of any project to ensure integrity of facilities in regard to code compliance.

7.4 Placement of cameras and cabling must be done in consideration of aesthetic elements in each case. This includes installation of conduit along walls and ceilings in older structures where drop ceilings are not available. Architectural and Engineering Services and other offices/departments, as may be appropriate, will be included in the planning phase of any project where aesthetic concerns are present.

7.5 No equipment, connection or other component of a surveillance camera system can be placed in any location or otherwise limit or negatively impact spaces controlled by UCO Information Technology without their permission pursuant to the design, installation and implementation procedure associated with this policy.

7.6 UCO Police will provide overall administration of system access rights to individuals in partnership with each department/division at the time of initial installation set up and as needed in the future. It is required that UCO know at all times who has access to view live and recorded images from each installed camera and that an administrative record is maintained in each case as part of the surveillance video management software.

- Authorization to view live or recorded images and permission to manage data created in this system must be established during the initial planning phases of installation inclusive of naming individual persons within the department that have these rights. Access rights will be managed exclusively by Police Services in partnership with the client departments. Any changes to access or management rights must be processed by the System Manager within Police Services. A person with granted rights to view and or operate cameras or view recorded images cannot transfer those rights to another person without coordination with Police Services. In no circumstance will any person with any level of access to a system allow another person to access or view camera images or share their system passwords with other individuals without permission of the appropriate department/division manager and in coordination with UCO Police Services.

7.7 No video surveillance system can be installed on campus without the additional following requirements (see also Video Surveillance Procedure):

- Written approval of Police Services and Information Technology as part of the planning phase of each respective project.
 - All newly requested installations will have an IT network impact assessment conducted as part of the planning procedure and the requesting department will not be allowed to proceed until the network can fully sustain and provide the level of service that is needed per direction of the Director of UCO Network Services or the Vice President of Information Technology.
- Written approval by the respective Vice President of the department/division making the request.
- Dedicated department/division budget resources to adequately fund the total cost of ownership of each respective installation.