**Procedure: Security Camera Deployment and Use**

Authority for Procedure granted by UWG PL 7009, Access Control and Security Systems Administration

Security Cameras are necessary to deter, detect and prosecute wrongdoing at the University of West Georgia (UWG). This procedure is necessary to ensure the effective, efficient, ethical, and legal deployment and use of UWG Security Cameras and their related Video Management Software (VMS) in:

- protecting sensitive or classified information;
- protecting UWG and personal resources;
- ensuring academic integrity;
- identifying those responsible for committing criminal acts;
- safeguarding and retaining video evidence, and;
- pursuing prosecution in accordance with federal and state law and Board of Regents (BOR) policy.

UWG employees, contractors, representatives, and others having responsibility or access to utilize VMS and Security Cameras leased or occupied by UWG or any entity with a UWG affiliation shall use said Security Cameras in a manner consistent with the federal and state law and this Procedure.

**Installation and Monitoring**

Security Cameras may be installed to enhance the security and safety of people or property. Cameras are limited to uses that do not violate the reasonable expectation of privacy as defined by law. Where appropriate, cameras may be placed campus-wide, inside and outside buildings. All camera installations are subject to federal and state laws.

Security Cameras shall not be installed with the intent to enforce University policy (e.g., workplace attendance, work quality, or academic conduct). Information obtained from Security Cameras in violation of this procedure shall not be used in a disciplinary proceeding against University students or employees. However, camera recordings captured during routine business may be utilized as a part of an investigation with reasonable cause or in a civil suit/other proceedings involving a person(s) whose activities are shown on the recording and relate to the proceeding. Reasonable cause may include but is not limited to suspicion or violations of University policy and state and/or federal laws.

Recorded images shall not be made public, nor shall recorded images be released to, provided to, or otherwise made accessible to any person, party, or entity without UPD’s express written permission or as required by law.

To request installation and/or monitoring access to a Security Camera, contact Access Control Services. Access Control, in coordination with Planning and Construction Services (PCS), Information Technology Services (ITS), and the Office of Legal Affairs (OLA), will ensure Security Cameras are placed and positioned so as not to compromise a person’s expectation of or legal right to privacy. Individuals are prohibited from installing and/or monitoring cameras or other intrusive electronic devices without express written permission from and coordination with UPD.

Information obtained from Security Cameras should be considered Confidential Data and must be handled with an appropriate level of security to protect against unauthorized access, alteration, or disclosure per UWG PL 5002, Data Security, and associated procedures.

All requests to obtain Security Camera recordings shall be submitted through the UPD Records Division or the Open Records Officer.

**Access and Monitoring of Security Cameras**
All university Security Camera recordings or monitoring of activities of individuals or groups will be conducted in a manner that is:

- Consistent with university policies and state and federal laws
- Professional, ethical, and legal
  - Personnel with access to university Security Cameras must be trained in monitoring equipment’s effective, legal, and ethical use.
- Not based on the subjects’ characteristics, including age, color, disability, gender, national origin, race, religion, sexual orientation, or other protected characteristics (see UWG PL 4002, Non-Discrimination and Anti-Harassment)

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 or 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, Security Camera access to live video or recorded video is limited to Authorized Persons, University Police, and other persons authorized by the Chief of Police or designee. All others may submit an open records request to request a copy or to inspect video footage at openrecords@westga.edu.

Exporting, copying, duplicating, or retransmission of live or recorded video is limited to persons within the University Police authorized by the Chief of Police.

Nothing in this section is intended to limit the authority of University Police or Access Control Services in law enforcement activities.

**Security Camera Functions**

Although the physical cameras may be identical, the security functions of these cameras fall into two main categories:

- **Property Protection** - The intent is to capture video and store it on a centralized video management system (VMS) so that if the property is reported stolen or damaged, the video may show the perpetrator (e.g., unstaffed computer or science lab, parking lot)

- **Personal Safety** - The intent is to capture video and store it on a centralized VMS so that if a person is assaulted, the video may show the perpetrator (e.g., public lounge, walkway, parking lot)

**Placement of Security Cameras**

The locations where Security Cameras are installed may be restricted access sites (e.g., departmental computer lab); however, these locations are not places where a person has a reasonable expectation of privacy. Cameras will be located to maximize personal privacy, and audio will not be recorded. Security Camera positions and views of residential housing will be limited. The view of a residential housing facility must not violate the standard of a reasonable expectation of privacy.

Monitoring by Security Cameras is prohibited in the following locations:

- Student living spaces in university residence halls and apartments
- Bathrooms
- Locker rooms
- Lactation rooms
● Health Services examination rooms
● Counseling Services session rooms

All video camera installations must be visible. Installation of “dummy” or placebo cameras that do not operate is prohibited.

Security Camera Requests

Units wanting Security Cameras installed in their area(s) need to contact Planning and Construction Services (PCS) and complete a WIC ticket by calling 678-839-6311 or emailing wic@westga.edu, or completing the online Service Request Form. PCS, UPD, ITS, and OLA will assess the location the cameras are wanted for necessity and legality of coverage as well as infrastructure and networking feasibility.

Once Security Cameras are approved, UPD will acquire a quote for the cameras, installation costs, licensing fees, and any related VMS from a Department of Administrative Services (DOAS) approved vendor. UPD will send the quote to the requesting party and liaise between the stakeholders and the vendor to reduce or expand the camera system and quote as needed.

*NOTE: Periodic maintenance and software update fees and annual licensing and decommissioning fees should be considered and budgeted for when the stakeholders are planning the Security Camera costs.*

Decommissioning

Access Control Services will oversee the installation, support, maintenance, replacement, and decommissioning of all approved Security Camera systems with the assistance of UPD, OLA, the appropriate Vice President, Information Technology Services, University Facilities, and external vendors as appropriate.

Funding

Security Cameras must be purchased with State funds. Research and UWG Foundation funds may not be used to purchase Security Cameras.

Applicability

Unless explicitly exempted, this procedure applies to all personnel, departments, colleges, campus organizations, subsidiaries, tenants, and public/private partnerships with the university for installing and using Security Cameras and their video monitoring and recording systems in any university-owned or leased spaces.

This procedure does not apply to:

● Security Cameras used inside University Police headquarters and sub-stations
● Mobile or hidden video equipment used in criminal investigations conducted by University Police
● Automated teller machines (ATMs), which may utilize cameras
● Cameras used for academic purposes
  ○ Cameras used for research are governed by policies involving human subjects
  ○ May not be used as a Security Camera or in another manner with the intent of circumventing this procedure
- Webcams for general use by university personnel (e.g., webcams installed on individual workstations, laptops, tablets, or cellular telephones) used for legitimate business purposes (e.g., video conferences)
  - May not be used as a Security Camera or in another manner with the intent of circumventing this procedure

- Use of video equipment to record public performances or events, sporting events, interviews, or other use for broadcast or educational purposes (e.g., videotaping athletic events for post-game review, videotaping concerts, plays, and lectures, or videotaped interviews)
  - May not be used as a Security Camera or in another manner to circumvent this procedure.

**Appropriate Use and Confidentiality**

Video Management System (VMS) users are prohibited from using or disseminating information acquired from University Security Cameras except for official purposes. All information or observations made using Security Cameras is considered confidential and can only be used for official University and law enforcement purposes.

To request access or monitoring rights, complete the [VMS Access Request form](#) and forward it to UPD - Access Control Services. Access Control will assess the Access Level needed and review justification and location requests. Access Control may approve or deny (in whole or in part) the request and inform the requesting party via written communication.

**Recordkeeping**

All appropriate measures must be taken to protect an individual’s right to privacy and secure University information through its creation, storage, transmission, use, and deletion.

Records will be maintained for the retention period, as stated in the USG [Records Retention Schedules](#) or state requirements, whichever is longer.

**Definitions**

**Access Level** - The authorization level required for any given access request depends on the lowest access level that will accomplish the operational purpose.

**Authorized Person** - UWG employees, currently enrolled students, and Affiliates possessing a duly issued and valid Access Credential permitting entry into University Facilities.

**Confidential** - information maintained by the institution that is exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws.

**Security Camera** - any item, system, camera, technology device, communications device, or process used alone or in conjunction with a network for gathering, monitoring, recording, or storing an image or images facilities and/or people. Such devices may include but are not limited to analog and digital security cameras, closed circuit television, and computerized visual monitoring.

**Unit** - Any college, department, program, research center, business service center, auxiliary service center, office, or other operating units.
Video Management System (VMS) - A video management system, also known as video management software plus a video management server, is a component of a Security Camera system that, in general:

- Collects video from cameras and other sources
- Records/stores that video to a storage device
- Provides an interface to both view the live video and access recorded video

Forms

- Work Information Center (WIC) Service Request Form
- VMS Access Request

Guidelines/Related material

FAQs on Photos and Videos under FERPA

USG Record Retention Schedules

Appendices/ Other Resources (i.e., training, checklists, job aids)