Video Monitoring and Surveillance Activities Policy

PURPOSE

The University of North Alabama 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 proper 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 UNA community. This policy addresses the University's desire to meet its 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.

SCOPE

This policy applies to all personnel, departments, and colleges of the University of North Alabama in the use of security cameras and 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:

1. *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.
2. *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.
3. *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 the video may or may not be recorded. Example: a computer lab with multiple rooms and only one member of staff.

Information obtained from the cameras shall be used for safety and security purposes and for law and policy enforcement, including, where appropriate, student conduct functions. However, prudence should be exercised by parties requesting such information to ensure that requests are limited to matters of substantial consequence. The availability of surveillance recordings does not remove the responsibility of supervisors to work to prevent, detect, and address issues as they should normally do. Information must be handled with an appropriate level of security to protect against unauthorized access, alteration, or disclosure.

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.

RESPONSIBILITIES

The University of North Alabama Police Department will manage all campus security surveillance systems pursuant to this policy.

To enhance security and aid law enforcement it may be appropriate to permanently install video devices on the campus. In such cases the following rules will apply:

- Individual departments, programs, or organizations wishing to permanently install video cameras shall submit a written request to the appropriate dean, director, or department head with a statement justifying the benefit of installing such equipment. The statement must include the proposed number and location of the device(s), as well as the purpose of the installation, whether the location of the cameras involve recording of activity by students, employees or the general public, and the name and title of the individual who will be responsible for reviewing the locations. The source of funding for the installation must be specifically identified as part of the request.
- The requesting department, program, or organization must work with the Information Technology Services, Facilities Administration and Planning, and the Chief of Police to determine the number and location of cameras prior to submitting their request.
- The appropriate dean, director or department head will forward the request along with his/her recommendation to their appropriate Vice President or if unavailable the Chief of Police.
- The Vice President or designee will review the request and will approve or disapprove. If approved the Vice President will forward the request to the University Executive Council with that recommendation.
- The University Executive Council in consultation with the Chief of Police, the Chief Information Officer, University's Legal Counsel, and the Assistant Vice President Facilities Administration and Planning shall be responsible for reviewing and approving or denying all proposals for security camera equipment recommended by a Vice President or the Chief of Police, and for approval of any requested exceptions to this policy.
- Unless otherwise directed by the University Executive Council, the Chief of Police for the University of North Alabama Police Department shall contact the Department of Facilities Administration and Planning and Department of Information Technology Services to oversee the installation of the video monitoring equipment. The Department of Facilities Administration and Planning will coordinate installation with a designated contractor or the Department of Information Technology Services. The contractor or Department of Information Technology Services will coordinate integration of the system.
- A member of the campus community may file a written request to change the location or limit the visual range of a specific installation of video monitoring equipment based on a belief that it infringes on a reasonable expectation of privacy or other protected rights. The request shall be submitted to the appropriate Vice President to the University Executive Council and shall (a) identify the location, (b) identify the right believed to be infringed, and (c) provide an explanation of how the video device installation infringes that right. The University Executive Committee will consult with the University's Legal Counsel and respond to the request within twenty (20) business days after receipt. The response will be based on a reconsideration of the initial request to install the devices in light of the campus community member's concerns. The decision of the University Executive Council is final.
- Within three months of the effective date of this Policy, all existing uses of video monitoring and recording equipment on campus shall be brought into compliance with all aspects of this policy, including the approval process outlined in the preceding paragraph. Those that do not conform shall be removed.

- No researcher or organization, whether faculty, staff, student, or the general public, is authorized to use these cameras or recordings from the cameras for research purposes.
- Monitors for video equipment shall be installed in controlled-access areas and shall not be viewable by unauthorized persons.

The University Police Department will manage all campus security surveillance systems pursuant to this policy.

The University Police Department and Information Technology Services (ITS) are responsible for implementation of this policy, specifically for the following.

- Advising departments on appropriate applications of surveillance technologies and providing technical assistance to departments regarding security camera systems.
- Monitoring 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.
- Reviewing proposals and recommendations for camera installations and specific camera locations to determine that the perimeter of view of fixed location cameras conforms to this policy and forwarding recommendations to the University Executive Council.
- Annually evaluating camera locations.
- Testing and maintaining the camera systems.

The University Police Department will review any complaints regarding the use of surveillance camera systems and determine whether this policy is being followed. The University Executive Committee will review appeals of decisions made by the Chief of Police.

The President or the University Executive Council, in consultation with University Legal Counsel, will review all external requests to release records obtained through security camera surveillance prior to the release of any records.

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.

Camera positions and views of residential housing shall be limited to public areas, elevators, and exterior locations. 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 – only at the entrance
- Classrooms not used as a lab

(These areas are protected by a "reasonable expectation of privacy." Use of cameras in these areas requires search warrants.)

The installation of “dummy” cameras that do not operate is prohibited. Unless being used for criminal investigations, all video camera installations should be visible.

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 and 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 shall be trained in the effective, legal, and ethical use of monitoring equipment and shall receive a copy of this policy and provide written acknowledgement that they have read and understand its contents.

Access to live video or recorded video from cameras shall be limited to the University Police Department, designated ITS personnel and other personnel as authorized by the Chief of Police and Executive Director of ITS. The copying, duplicating and/or retransmission of live or recorded video shall be limited to persons authorized by the Chief of Police.

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.

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.

Any use of security cameras for reasons other than those cited in this policy is strictly prohibited. Violations of this policy or the procedures outlined therein will result in disciplinary actions consistent with the rules and regulations governing employees and students of the University as found in the Student Handbook and Employee Handbook.

USE OF CAMERAS FOR CRIMINAL INVESTIGATIONS

Mobile or hidden video equipment may be used in criminal investigations by the University Police Department. Covert video equipment may also be used for non-criminal investigations of specific instances that may be a significant risk to public safety, security and property as authorized by the Chief of Police.

USE OF CAMERAS FOR NON-CRIMINAL INVESTIGATIONS

Covert video equipment may be used for non-criminal investigations of specific instances that may be a significant risk to public safety, security, and property as authorized by the Chief of Police. An example of a non-criminal investigation would be an internal investigation conducted for HR where the goal is not to prosecute, but to determine continued employment after inappropriate use of university equipment or resources has been discovered. Another example would be video obtained to enforce a University policy and procedure such as students propping open doors in a residence hall (not illegal, but a definite violation of policy).

EXCEPTIONS

This policy does not apply to cameras used for academic purposes. Cameras that are used for research are 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. 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 include videotaping of athletic

events for post-game review, videotaping of concerts, plays, and lectures, or videotaped interviews of persons. Automated teller machines (ATMs) that use cameras are exempt from this policy.

REQUEST FOR ACCESS TO LIVE AND/OR RECORDED VIDEO

Individual colleges, departments, programs, or campus organizations wishing to have access to live and/or recorded video shall submit a written request to the appropriate Vice President describing the requested access, with justification.

- The Vice President will review the request in consultation with the Chief of Police, if appropriate, and will forward it to the University Executive Council with a recommendation.
- The University Executive Council shall be responsible for reviewing and approving or denying all access requests recommended by the Chief of Police, via the Vice President.

TRAINING OF CAMERA OPERATORS

The University Police Department and the Information Technology Services department shall train camera operators 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 understand its contents.

STORAGE AND RETENTION OF RECORDINGS

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

All surveillance recordings shall be stored in a secure location for a period of 30 days and will then be erased or written over, unless retained as part of a criminal investigation, a civil or criminal court proceeding, or pursuant to a Preservation Notice issued by the University's legal counsel.

- Recordings will be stored in a manner consistent with available technology and transported in a manner that preserves security. Both current and archived recordings will be secured. All storage and access to recordings will be controlled by the University Police Department. Surveillance records shall not be stored by individual departments.
- Recordings used in law enforcement investigations or criminal prosecutions shall be retained until the end of the court or judicial proceedings and appeal period unless directed otherwise by a court.
- Recordings may also be retained for other bona fide reasons as determined by the University Police Department, in consultation with the University's legal counsel.
- Recordings shall be retained for 30 days and then will be erased or recorded over unless retained as part of a criminal investigation, a civil or criminal court proceeding, pursuant to a Preservation Notice issued by the University's Legal Counsel. No attempt shall ever be made to alter any recording. Editing or otherwise altering recordings or still images, except to enhance quality for investigative purposes or blur features as described above, is strictly prohibited.
- Transmission of recordings using the Internet or campus network will use encryption technology to ensure that recordings are not improperly accessed.
- For FERPA purposes, recordings with information about a specific student are considered law enforcement records unless the University uses the recording for discipline purposes or makes the recording part of the educational record.
- The deletion of video, pursuant to this policy, and any exemption to the policy on deletion and records storage must be approved by the University Executive Council.

- Only the Chief of Police and the Chief Information Officer of the University are to be permitted and have the ability to delete video recordings pursuant to this policy.
- Individual departments shall not store video surveillance recordings.
- Editing or otherwise altering recordings or still images, except to enhance quality for investigative purposes or blur features as described above, is strictly prohibited.

A log shall be maintained by the Chief of Police 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. The Chief of Police will also maintain a list of personnel approved to monitor live and/or recorded video feeds, with validation of each person having completed the required training. The right to view anything but live video will be very limited to ensure the integrity of this policy.

DESTRUCTION OR TAMPERING WITH CAMERAS

Any person who tampers with or destroys a camera or any part of the electronic surveillance system may be prosecuted in the criminal justice system as well as the campus Student Conduct system.

Approved by the Shared Governance Executive Committee and the President, 03/07/2016.
Revised and Approved by the Shared Governance Executive Committee and the President, 02/19/2020.
Revised and Approved by Shared Governance the President, December 2022.