

Policy Number: 1.23 Policy Level: Operating Policy Originally Issued: February 19, 2018

> Reviewed: April 1, 2020 Reviewed: August 3, 2022

Policy Owner: Vice President for Financial Affairs Policy Implementation: Chief of Security

Security Camera and Video Surveillance

I. Policy Statement and Purpose

Athens State University is committed to providing a safe environment and enhancing the quality of campus life by integrating the best practices of safety and security with technology. A vital component of a comprehensive security plan is the utilization of a security and video surveillance system. The surveillance of public areas is intended to deter crime and assist in protecting the safety and property of the campus community. The purpose of this policy addresses procedures for installation of security camera and video surveillance equipment and the handling, viewing, retention, dissemination, and destruction of surveillance records.

II. Installation Procedures and Locations

Security cameras and video surveillance equipment may only be installed and maintained at locations that have been approved by the Vice President for Financial Affairs, upon the vice president's determination that the security and/or safety of persons or property would be enhanced by the use of that location. Such cameras may be located campus-wide, inside and outside of buildings. All security cameras and video surveillance equipment must be connected to the same secure University network.

Several of the security cameras on University property have audio capabilities, and while the audio capabilities are generally disconnected, persons should be on notice that they may be enabled for special events or situations. By way of example but not as a limitation, such occasions could include events with numerous guests from off-campus (such as The Old Time Fiddlers Convention), or situations where there has been an indication of a threat to persons or property. However, the audio capabilities will not be used in a manner that violates Alabama law.

III. Monitoring

Employees of Athens State University are prohibited from utilizing the security cameras for personal reasons unrelated to the legitimate business operations of the University, in a manner that violates reasonable expectations of privacy, as defined under Alabama law, or in a manner that is not consistent with University policies and guidelines, including those that address nondiscrimination



Policy Number: 1.23 Policy Level: Operating Policy Originally Issued: February 19, 2018

> Reviewed: April 1, 2020 Reviewed: August 3, 2022

Policy Owner: Vice President for Financial Affairs Policy Implementation: Chief of Security

harassment, and sexual misconduct. Employees are subject to disciplinary action, ranging from oral reprimand to dismissal from employment, for the violation of this policy.

There may be instances when University departments or employees in those departments need access to monitor certain cameras/video surveillance equipment for personal work area safety and security related to their particular department (i.e., such as front doors of Chasteen Hall and the AMSTI building, isolated hallways leading to offices). In those cases, the departments or employees may request this access by completing the <u>Security Camera and Video Surveillance Request to Monitor</u> form. This form must be approved by the Vice President for Financial Affairs before monitoring access is granted.

Persons are on notice that University security cameras may be placed in all parts of University owned and/or controlled property and locations. (Appropriate signage will be placed at camera locations where such signage is deemed by the University to be practical and effective, but signage may not be deemed practical and effective in all areas.) However, unless the security cameras are being used in connection with investigations relating to suspected criminal activity, monitoring by security cameras in the following locations is prohibited: (1) bathrooms, (2) offices, and (3) classrooms that are not used as a lab. Also, unless being used in connection with investigations relating to suspected criminal activity, all video camera installations must be visible.

The University does not guarantee or provide any assurance that security cameras will be monitored in real time, 24 hours a day, but the University reserves the right to do so. Generally speaking, security cameras are viewed on a periodic basis or in response to a specific incident, but the University may view them in a different manner given the circumstances.

IV. Retention, Dissemination and Destruction of Surveillance Records

All security cameras are capable of recording images continuously. All information and/or observations collected through the use of security cameras are considered University property and/or records that are sensitive, confidential and can only be used for official university and law enforcement purposes. Recorded video will generally be retained for a minimum of fourteen (14) days, although recordings that are more than 14 days old may be retained for university business, criminal and/or judicial investigation purposes. Video recordings for such purposes will be stored in a secure location with access by authorized personnel only.



Policy Number: 1.23 Policy Level: Operating Policy Originally Issued: February 19, 2018

> Reviewed: April 1, 2020 Reviewed: August 3, 2022

Policy Owner: Vice President for Financial Affairs Policy Implementation: Chief of Security

All requests from external sources for the release of information must be submitted to and approved by the Chief of Security and the Vice President for Financial Affairs. All dissemination must be authorized by the Chief of Security and the Vice President for Financial Affairs.

V. Exceptions

This policy does not address the use of webcams for general use by the University. This policy 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 (*i.e.*, concerts, plays, and lectures, or videotaped interview of persons).

This policy does not apply to cameras used for academic purposes. Cameras that are used for research would be governed by other policies involving human subjects and are, therefore, excluded from this policy.

This policy also does not apply to mobile video equipment operated by law enforcement personnel, recordings required by court order or subpoena, or portable hidden cameras with recording equipment used for criminal investigations by law enforcement personnel.

VI. Responsibility for this Operating Policy

Policy Owner

As part of the initial approval of this policy by the President and subsequent to the original dissemination of the policy, the Vice President for Financial Affairs is the policy owner for the ongoing evaluation, review, and approval of this policy. Subsequent reviews and revisions to this policy must be in accordance with approved operating policy procedures and processes.

This policy will be reviewed every two years or more frequently as needed by the Policy Owner. Revisions will be reviewed/affirmed by the Faculty Senate and the Cabinet and approved by the University President. This policy will be updated/published in the University's Policy Library.

Responsibility for Policy Implementation

The President has assigned the responsibility of implementing this policy to the Chief of Security.