[New Policy: July 2, 2019]

Angelo State University
Operating Policy and Procedure

OP 62.05: Video Security/Surveillance Systems

DATE: July 2, 2019

PURPOSE: It is the policy of Angelo State University to manage the use of and access to video recording security systems so that safety and security is enhanced while respecting individual's privacy rights.

REVIEW: This OP will be reviewed in January every five years, or as needed, by the Campus Security Camera Advisory Committee with recommended revisions forwarded through the vice president for finance and administration to the president by February 15 of the same year.

POLICY/PROCEDURE

1. Definition

ASU defines technical policy terms in the glossary.

2. Scope & Audience

a. This policy applies to all employees and students with respect to the installation and use of video security cameras, except as noted below, in facilities owned or controlled by the university.

b. All references to video security systems throughout this policy are for those systems which were designed and installed with the intent and ability to record video and/or to be monitored for purposes of enhancing campus safety and physical facility security.

c. This policy governs all video monitoring systems with planned installation following the policy's effective date. Existing installations and written procedures for the use of those existing video monitoring and recording systems shall be brought into compliance with this policy by December 31, 2019.

d. Exclusions

This policy does not apply to:

(1) Use of video recording technology covered by university policies governing research with human subjects or animals.

(2) Use of video recording technology for video conferencing.

(3) Use of class lecture/test recordings and/or archiving for the purpose of content sharing.

(4) The academic use of non-security cameras for educational purposes.

(5) Construction site time-lapse cameras.

(6) Use of video/audio recording systems used by the Angelo State University Police Department ("UPD"). The UPD must comply with existing police department operational policies for use of these systems.

3. Responsibilities & Procedures

When deploying video security systems on campus, all individuals granted access to those systems are required to abide by the responsibilities and procedures set forth in this policy.

a. Purpose for Use of Monitoring Systems

The purpose of video monitoring governed by this policy is for enhanced safety and security. Any interception, duplication, transmission, or other diversion of video technologies for purposes other than the safety and security contemplated by this policy is strictly prohibited.

Safety and security purposes include, but are not limited to:

(1) Protection of individuals, including students, faculty, staff, and visitors.

(2) Protection of university owned and/or operated property and buildings, including building perimeters, entrances and exits, lobbies and corridors, receiving docks, special storage areas, laboratories, and cashier locations.

(3) Monitoring of common areas and areas accessible to the public, including transit stops, parking lots, public streets, and pedestrian walks.

(4) Investigation of criminal activity.

(5) Protection against an act of terrorism or related criminal activity.

(6) Protection of Critical Infrastructure as defined under the Texas Homeland Security Act, the USA Patriot Act, or the United States Department of Homeland Security.

(7) Any department seeking a copy of security camera video footage for investigative purposes must obtain prior authorization from the chief of police. Requests for copies of security footage may be denied if such request could jeopardize a criminal investigation or hinder the prosecution of a criminal case.

b. Monitoring System Protocol

(1) Video monitoring and recording are required to be conducted in accordance with all existing university policies. Monitoring based solely on the characteristics and classifications contained in the Non-Discrimination Policy (e.g., race, gender, sexual orientation, national origin, disability, etc.) is prohibited.

(2) Monitoring or recording of audio is strictly prohibited. The interception of oral communications without court authority is a violation of United States Code, Title 18, Section 2511 ("Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited").

(3) Monitoring shall be limited to uses that do not violate a reasonable expectation to privacy.

(4) Cameras may be monitored in real time, but cameras may also be unmonitored while recording.

(5) Violations of the responsibilities and procedures set forth under Section 4 of this policy may result in disciplinary action consistent with the rules and regulations governing employees of the university.

c. Monitoring System Usage Requirements

(1) The Campus Security Camera Advisory Committee is authorized to oversee the use of video monitoring for safety and security purposes at the university.

(2) The Campus Security Camera Advisory Committee will be responsible for reviewing and approving or denying all proposals for security camera access/equipment. The Campus Security Committee shall be responsible for the review and approval of any requested exceptions to this policy.

(3) The Campus Security Camera Advisory Committee shall be comprised of seven members;

(a) chief of police or designee, chair campus security camera advisory committee

(b) director of human resources or designee

(c) vice president for student affairs and enrollment management or designee

(d) vice president for academic affairs or designee

(e) vice president for finance and administration or designee

(f) director of risk and emergency management or designee

(g) chief information officer, information security officer or designee

(4) Temporary installation of video monitoring systems:

(a) The chief of police has the responsibility to authorize any temporary installation as deemed necessary in connection with a criminal investigation, for enhanced security.

(b) Temporary cameras must be removed once investigations are concluded.

(5) If a camera is proposed or is installed in a research space, an authorized representative from the Office of Sponsored Projects ("OSP") must approve the

location and ensure a "Technology Control Plan" has been established, if applicable. Installation of video equipment is prohibited in restricted areas where Department of Defense classified information is discussed, stored or otherwise processed without the approval from the vice president for academic affairs, or his/her designee.

(6) All operators and supervisors involved in video surveillance are required to perform their duties in accordance with this policy.

(7) Personnel involved in monitoring and recording must complete Blackboard training prior to being given access to the camera security system. Annual training is required to maintain access to the camera system.

(8) All Camera Operators:

(a) Must not monitor individuals based on characteristics of race, gender, ethnicity, sexual orientation, disability, or other classifications protected by the university's Non-Discrimination Policy.

(b) Must not view places where people have a right to privacy, including but not limited to bathrooms, dressing rooms, locker rooms, private rooms or areas through windows.

(9) Installation of cameras with audio recording capability is prohibited.

(10) No video security system may be accessible from the public internet.

(11) All video systems and locations are required to be coordinated/installed by Information Technology.

d. Records Retention

(1) Recordings must be retained in a secure location with access by authorized personnel only.

(2) Security recordings are stored for 30 days before being purged.

e. Requests for Information Obtained from Monitoring Systems

(1) Release of recorded video must be approved by chief of police.