Security Camera Policy **Reviewed July 5, 2018**

Purpose

- ACOM is committed to enhancing the quality of life of the campus community by integrating the best practices of safety and security with technology. We have added security cameras to a portion of our campus to assist in making our campus as safe as possible. The deployment of cameras is supported by the administration. The Director of Operations per the Dean's Cabinet is responsible for the oversight and approval of camera locations.
- Protect the security of ACOM's Campus.
- These cameras are actively monitored and they are intended to deter crime and assist in investigation of crimes and recovery. This policy addresses the College's safety and security needs while respecting and preserving individual privacy.
- To ensure the protection of individual privacy rights in accordance with the College's 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. Policy All video footage will be secured and will be managed by the Director of Operation with technical support provided by the Information Systems department. Any requests to view camera footage will be submitted to the Office of the Dean.
- The Security Department shall monitor 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.
- The Dean's Cabinet will review proposals and recommendations for camera installations and review specific camera locations to determine that the perimeter of view of fixed location cameras conforms to this policy.
- The Director of Operations will review any complaints regarding the utilization of surveillance camera systems and determine whether this policy is being followed.
- The Director of Operations will review all external requests to release records obtained through security camera surveillance. The College will seek consultation and advice from the General Counsel as needed related to these requests prior to the release of any records outside of the College. Video surveillance records will generally not be released to the public, students, general employee, and parent or law enforcement agency. The content of the video is a College record subject to administrative regulations regarding confidential student records. While College personnel will typically review the footage, the College reserves the right to allow individuals to view video footage if that is a necessary action as part of an investigation of a crime, code of conduct violation, significant campus safety concern or campus policy violation.

Scope

Policy

Authority, Standards, and Access

The Director of Information Systems - ACOM or designee is responsible for establishing and enforcing all Print resources. Any print installation or use that varies from this standard must be approved by the DIS-ACOM.

Security Camera Policy **Reviewed July 5, 2018**

General Principles

Cameras are actively monitored. They are viewed upon report of a crime or violation.

Information obtained from the cameras shall be used exclusively for campus policy enforcement, including, where appropriate, student judicial functions or to assist local law enforcement and campus/local crime. 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 College information securely through its creation, storage, transmission, use, and deletion.

All camera installations are subject to federal and state laws. Placement of Cameras Cameras will be located so that personal privacy is protected.

No audio shall be recorded. Camera positions and views of residential housing shall be limited to external areas. The view of a residential housing facility must not violate the standard of a reasonable expectation of privacy.

All video camera installations should be visible. The exact location, number and function of all cameras will generally be considered confidential for security purposes and not be released to the general public, guests or employees. The College reserves the right to place cameras in areas that are not open to the campus or general public (as example closed buildings or secured areas).

Anyone who tampers with video equipment will be subject to disciplinary action through the Dean of Students office. Access and Monitoring All recording or monitoring of activities of individuals or groups by college security cameras will be conducted in a manner consistent with College policies, 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 college security cameras should be trained in the effective, legal, and ethical use of monitoring equipment.

When an incident is reported, the personnel responsible for the area in question may request the Public Safety to review the images from the camera. As circumstances require, the Director of Operations may authorize others to review images. A log will be kept of all instances of access to, and use of, recorded material. This log will be discarded at the end of each academic year. Appropriate Use and Confidentiality 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 college and law enforcement purposes upon the approval of the Director of Operations or designee. Personnel are expected to know and follow this policy.

Use of Cameras for Criminal Investigations: The use of video equipment may be used in criminal investigations on behalf of the College. Individuals or agencies from outside of the College must request access to view materials in accordance with our policies governing student records. Video records will be destroyed within seven days at the conclusion of any investigation and subsequent hearing process. Exceptions This policy does not apply to cameras used for academic purposes. Cameras that are used for

research, communications, class projects or Communication's department organizations would be governed by other policies involving human subjects and are, therefore, excluded from this policy. Safety and Security Camera Acceptable Use Policy This policy does not address the use of student/employee personal cameras Webcams, videotaping events, live streaming for general use by the college. 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 would include videotaping of athletic events for post-game review, videotaping of concerts, plays, and lectures, live stream activity or videotaped interviews of persons. Automated teller machines (ATMs), which may utilize cameras, are also exempt from this policy. Procedures Departments requesting security cameras will be required to follow the procedures outlined in this policy. Training Camera control operators shall be trained in the technical, legal, and ethical parameters of appropriate camera use. Camera control operators shall receive a copy of this policy and provide written acknowledgment that they have read and understood its contents. Operation Video surveillance will be conducted in a manner consistent with all existing university policies. Camera control operators shall monitor based on suspicious behavior, not individual characteristics. Camera control operators shall not view private rooms or areas through windows. All operators and supervisors involved in video surveillance will perform their duties in accordance with this policy. Abuse of standard operation policies or inappropriate camera control operations will result in disciplinary action. Storage and Retention of Recordings No attempt shall be made to alter any part of any surveillance recording. Surveillance centers and monitors will be configured to prevent camera operators from tampering with or duplicating recorded information.

All surveillance records shall be stored in a secure location for a period of 21 days and will then promptly be erased or written over, unless retained as part of a criminal investigation or court proceedings (criminal or civil), or other bona fide use as approved by the Director of Operations. Individual departments shall not store video surveillance recordings.

A log shall be maintained 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.

Interference

None

Questions

Questions regarding this policy should be sent to Director of Information Systems – ACOM at support@acom.edu.