

Policy Title:	Security Cameras
---------------	------------------

Governing Body:	Finance and Administration	Policy Number:	FAD.045
Policy Contact:	Director, Campus Public Safety	Date Revised:	
Custodial Office:	Campus Public Safety	Date Approved:	4/11/2016
Approved By:	President/Cabinet	Next Review:	
Related Policy:			

A. Purpose

To regulate the purchase, installment, use of security cameras and, security monitoring in order to standardized camera use while protecting the legal and privacy interests of the University and the University community.

B. Definitions

- **Private Work Space:** An employee’s exclusive private office, desk, and file cabinets containing personal matters not shared with other workers.
- **Private Space:** Places where people have a right to privacy, including but not limited to bathrooms, dressing rooms, locker rooms, and residence hall rooms.
- **Security Camera:** Any item, system, camera, technology device, communications device, or process, used alone or in conjunction with a network, for the purpose of gathering, monitoring, recording or storing an image or images of university facilities and/or people in university facilities. Images captured by security cameras may be real-time or preserved for review at a later date. Such devices may include, but are not limited to the following: close circuit television, web cameras, real-time security camera systems, and computerized visual monitoring.
- **Security Camera Monitoring or Recording:** The process of using a security camera to observe, review or store visual images for purposes of deterring crime, enhancing personal safety, protecting property, and solving criminal investigations.
- **Security Review Panel:** A group comprised of the Vice President for Finance and Administration (or his/her designee), Director of Public Safety, Director of Human Resources (or his/her designee), Chief Information Officer (or his/her designee), Student Conduct Coordinator (or his/her designee) and a Student representative.
- **University Facilities:** All University space on University owned, leased or controlled property, both internal and external, and includes all buildings, offices, common spaces, labs, grounds, and all other spaces.

C. Policy Statement

The use and deployment of security camera systems is to enhance the safety of the campus community and to protect university property in support of the University’s mission.

This policy applies to all employees and students with respect to the installation and use of security cameras, except as noted, in University facilities.

All security cameras will only be installed with the advance approval of the Vice President for Finance and Administration with the Security Review Panel (“Panel”) recommendation as defined by this policy. Only authorized personnel, as determined by the Vice President for Finance and the Panel, will be involved in, or have access to, stored security camera data.

This policy does not apply to:

1. Use of video recording for research with human subjects or animals.
2. Use of video recording for video conferencing.
3. Use of video recording of events and performances.
3. Use of class lecture recordings and/or archiving for the purpose of content sharing.
4. Use of video recording for the purpose of providing accommodations for persons with disabilities.
4. Use of mobile video/audio recording systems used by Campus Public Safety.
5. Use of video recording performed by non-University personnel.

Installation of new security cameras must be approved in advance by the Security Review Panel and the Vice President for Finance and Administration. Once approved, security camera systems must connect to a centralized university system maintained by the Department of Information Technology.

Security cameras will be installed and configured to prevent tampering with or unauthorized duplicating of recorded information. Security cameras will not record sound.

The conduct of security camera monitoring or recording, and the use of security cameras, must be in a manner consistent with all University administrative policies and procedures. The use of security cameras at the University are limited to uses that do not violate federal or state constitutional protections against unreasonable search and seizure or other applicable laws including federal and state laws prohibiting wiretapping and electronic surveillance of aural communications.

The Security Review Panel will limit camera positions. Any view will be no greater than what is available with unaided vision.

Images obtained through security camera recording must be retained for a length of time deemed appropriate for the purpose of monitoring, but not to exceed 90 days, unless such images have historical value, or are being used for a criminal investigation in accordance with this policy. Campus Public Safety must be involved when recordings are being retrieved for criminal investigations except when Campus Public Safety is the subject of that criminal investigation.

Using video recordings to monitor an employee’s or a student’s activities and/or the placement of camera’s in private spaces without the employee’s or student’s knowledge is prohibited. Information unlawfully obtained in violation of this policy shall not be used in any disciplinary proceeding against any University employee or student. Any employee violating this policy may be disciplined, up to and including termination under relevant provisions of collective bargaining agreements.

Only authorized personnel, as determined by this policy and authorized by the Security Review Panel will be involved in, or have access to security camera data.

1. Campus Public Safety will have access to all security camera data when it involves a criminal investigation
2. Criminal investigation information captured by the University Camera system can be shared by Campus Public Safety Directors with the Department of Human Resources, Provost’s Office and/or a request from

legal staff. Investigation information captured at the Higher Education Center may be shared with appropriate Rogue Community College personnel.

EXISTING CAMERA SYSTEMS

Managers for all existing systems installed prior to the issuance of this policy must submit a **Security Camera Location Document** (See Camera Procedures-Appendix A) to Campus Public Safety.

Images obtained through camera systems in place prior to DATE POLICY ADOPTED that are not connected to a central server maintained by the Department of Information shall be responsible for the maintaining of their recorded data for at least 30 days, but not more than 90 days. When these cameras are replaced, they must be converted to the centralized university camera security system.

This policy may be revised at any time without notice. All revisions supersede prior policy and are effective immediately upon approval.

D. Policy Consultation

Cabinet, Business Affairs Committee, Faculty Senate, Policy Committee, Provost's Advisory Committee

E. Other Information

Responsibilities of Security Review Panel

- Reviews all requests for installation and/or placement of security cameras.
- Reviews complaints regarding security camera locations and determines whether the policy is being appropriately followed. Periodically reviews existing camera locations to ensure that the placement of fixed location security cameras conforms to this policy.
- Provides a copy of this policy to managers or supervisors involved in security camera monitoring and recording.

Supervisors of Operators Involved in Security Camera Monitoring and Recording

- Provide a copy of this policy to any camera operator.

All Operators Involved in Security Camera Monitoring and Recording

- Receive a copy of this policy and provide written acknowledgement that they have read and understood its contents and will perform their duties in accordance with this policy.

The Policy Contact, defined above, will write and maintain the procedures related to this policy and these procedures will be made available within the Custodial Office.