Policy # 4312
Campus Video Surveillance

Date of Current Revision: August 2019
Responsible Officer: Associate Vice President for Business Services

---

1. PURPOSE

This policy provides guidelines for implementation and use of campus video surveillance.

2. AUTHORITY

The Board of Visitors has been authorized by the Commonwealth of Virginia to govern James Madison University. See Code of Virginia § 23.1-1600; § 23.1-1301. The Board has delegated the authority to manage the university to the president.

STATE OR FEDERAL STATUE AND/OR REGULATION

The Virginia Public Records Act (Code of Virginia §42.1-76 et. seq.) governs storage, retention and disposal of video recordings.

3. DEFINITIONS

Centralized Surveillance System
A system wherein network cameras require a central video server to receive all recordings from the platform via Internet Protocol. Cameras connected this system can have recording functions take place locally or remotely, allowing collection of this data away from or off site from individual camera locations.

Digital Video Surveillance System
An appliance that enables embedded image capture capabilities that allows video images or extracted information to be compressed, stored or transmitted over communication networks or digital data links. Digital video surveillance systems are used for any type of monitoring.

Video Surveillance System
A system of monitoring activity in an area or building using a television system in which signals are transmitted from a camera to receivers or servers by cables, telephone or wireless data links forming a closed circuit.

4. APPLICABILITY

This policy applies to all university administrators, faculty, staff, students and visitors.

5. POLICY

James Madison University reserves the right to place video surveillance cameras on campus where it deems necessary and appropriate. James Madison University respects the right to privacy of the university community members and balances the right to privacy with the safety needs of the campus community. JMU security cameras are not generally monitored continuously under normal operating conditions but may be monitored for legitimate safety and security purposes that include, but are not limited to; high risk areas, restricted access areas/locations, alarm responses, special events,

maintenance purposes, functionality purposes and specific investigations authorized by the senior vice president for administration and finance or designee.

6. PROCEDURES

A. Access and Use:

1. Only authorized personnel, as determined by this policy and authorized by the director of public safety or designee, will be involved in or have access to surveillance camera data.
2. The use of dummy or placebo cameras is prohibited.
3. University police will have access to all surveillance camera data from the department of public safety office location, or satellite locations as designed or designated.
4. When an incident is suspected to have occurred, only authorized personnel may review the images from surveillance camera data.
5. Only the director of public safety or his/her designee may authorize copies of surveillance images.
6. Personnel are prohibited from using or disseminating information acquired from campus video surveillance 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 upon the approval of the director of public safety or designee. Personnel are expected to know and follow this policy. All requests for release of surveillance records must be authorized by the university counsel and the director of public safety.
7. In general, the university will not permit the use or installation of cameras, personal webcams or similar technology as a tool to monitor routine performance or management issues involving university personnel. Employees of any department with surveillance cameras shall be notified of such installation.
8. Only authorized personnel may install, move or modify surveillance equipment.
9. Video monitoring normally will not be conducted in areas where there is a reasonable expectation of privacy.
10. The use of mobile or hidden video equipment may be used in criminal investigations. Covert video equipment may also be used for criminal investigations of specific instances which may be a significant risk to public safety, security, and property as authorized by the Senior Vice President for Administration and Finance or designee.
11. Video surveillance cameras shall not be specifically directed or zoomed into windows of any residential building, including residence halls. Electronic shielding or other methods will be used to ensure cameras do not have the ability to look into windows.
12. Proposed changes or exceptions to the Campus Video Surveillance policy will be reviewed by the director of public safety and building safety technologies staff on an annual basis.

B. Data and Access Log Storage:

1. Recorded camera images will be retained for at least 14 days or more; therefore, all purchased devices must be capable of retaining media for at least this period of time.
2. A log documenting access to and use of data stored in the university's centralized surveillance system will be maintained for a period of 12 months.
3. All records generated by and related to campus video surveillance shall be stored, retained and destroyed in compliance with applicable Library of Virginia records retention and disposition schedules.

C. Device Procurement, Installation, and Maintenance:

1. The installation of new surveillance cameras, their locations, and purpose must be approved in advance by Facilities Management's Building Safety Technologies staff. A request for surveillance camera installation must be submitted through Facilities Management Work Control (568-6106) using

the AIM system. A request for an estimate must be submitted as the first step in the installation request process.
2. Surveillance cameras must be compatible with and connect to the university's centralized surveillance system under the responsibility of building safety technologies, in accordance with university product, installation, maintenance, and support standards.
3. All costs associated with the purchase, installation, and maintenance of the system will be the responsibility of the requesting department.
4. All existing surveillance cameras must be connected to the university's centralized video surveillance system by September 1, 2018 or risk removal of equipment. Requests for exemption should be submitted to and will be considered by building safety technologies.
5. All authorized cameras and systems will be inspected annually to ensure that they are in proper working condition and meet policy guidelines.

7. RESPONSIBILITIES

Vice presidents are responsible for ensuring that their respective divisions are implementing the policy properly and that Facilities Management is informed as to the need for specific installations and repairs to installed systems. Academic unit heads and administrative department heads are primarily responsible for notifying Facilities Management as to the specific requirements of an installation and informing Facilities Management's Maintenance Control when installed systems are not working properly. In the event the camera system needs to be upgraded, the associated costs are the responsibility of the department. Facilities Management will be directly responsible for assigning building safety technologies to perform installation and preventative maintenance to installed systems and repair of inoperative systems, as well as removal of improper or incompatible systems. Building safety technologies will ensure that systems are functioning as designed and upgraded as needed to maintain overall compatibility and system integrity.

All departments, offices and employees that generate, receive or maintain public records under the terms of this policy are also responsible for compliance with Policy 1109 - Records Management.

8. SANCTIONS

Sanctions will be commensurate with the severity and/or frequency of the offense and may include termination of employment or expulsion in the case of students.

9. EXCLUSIONS

This policy does not address the use of student/employee personal cameras, and/or webcams, videotaping events or live streaming 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 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.

This policy does not apply to cameras used for academic purposes. Cameras that are used for research, communications, class assignments or projects conducted by university sponsored educational organizations would be governed by other policies involving instructional activities and are therefore excluded from this policy.

10. INTERPRETATION

The authority to interpret this policy rests with the president and is generally delegated to the associate vice president for business services.

Previous version: N/A
Approved by the President: N/A