Missouri Western State University

Policy Name: Campus Surveillance System	**Responsible Office:** Risk Management
Policy Category: Safety and Risk Management	**Approval Authority**: Vice President of Finance and Administration
Date Effective: May 26, 2026	**Date Last Reviewed/Revised:**

I. Purpose

The purpose of this policy is to establish guidelines for the use, management, and access control of camera systems deployed on the University's campus. This policy aims to enhance security, protect privacy, and ensure compliance with relevant laws and regulations, while upholding principles of confidentiality and ethical conduct.

II. Applicability

This policy applies to all University-owned camera systems deployed on campus premises, including those used for security monitoring, surveillance, and other purposes. All personnel, departments, colleges, campus organizations, public/private partnerships with the University, subsidiaries, and tenants are subject to this policy unless specifically exempted.

This policy does *not* apply to:

- Policy body cameras worn by members of the University Police Department (UPD), UPD vehicle or dash cameras, or recordings of interrogations conducted by UPD.
- Covert video equipment used for non-criminal investigations of specific instances that may pose a significant risk to public safety, security, and/or property as authorized by the UPD Chief or designee; however, the use of such cameras shall remain subject to applicable state and federal laws as well as the internal policies and procedures of UPD.
- Cameras used for academic purposes where notice has been given that video or audio recording is occurring.
- Cameras used for research that is regulated by the University's Institutional Review Board or the Institutional Animal Care and Use Committee.
- General web broadcasts made by the University, such as commencement, state of the University addresses, or meetings of the Board of Governors.
- Recordings of public performances, events, or interviews for broadcasts, such as athletic events, concerts, plays, or lectures.
- ATMs with video cameras.
- Cameras used for video conferencing and/or cameras attached to individual computers when used for legitimate business purposes.

III. Definitions

RBAC/RBAC Model: Role-Based Access Control: A system for restricting system access to authorized users based on their role within the organization. Access permissions are granted according to specific operational responsibilities.

Camera System: For the purposes of this policy, the term refers to University-managed centralized security camera systems operated by Risk Management, Technology Services, and the University Police Department. This excludes department-specific or academic/research-based camera systems unless otherwise noted.

IV. Policy

The University deploys surveillance systems for the purposes of enhancing campus security, deterring criminal activity, and promoting a safe and secure environment for all members of the University community. Camera footage may be used for security monitoring, incident investigation, and the collection of evidence in accordance with this policy and applicable laws and regulations.

Security surveillance installations are subject to compliance with all relevant federal, state, and local laws, ensuring that the use of cameras does not infringe upon reasonable expectations of privacy as defined by law. Cameras/surveillance systems may be installed in both indoor and outdoor locations across campus to fulfill the following objectives:

- **Deterrence of criminal activities:** Enhance campus safety by discouraging potential threats.
- **Monitoring and investigation:** Support incident investigations and provide evidence as needed.
- **Protection of property:** Safeguard University assets and resources.
- **Extended responsibility:** Cameras may provide live-stream monitoring by staff in nearby locations, such as food service areas or testing centers, to support limited staffing and enhance supervision.

Cameras and surveillance systems will not be installed for the purpose of conducting personnel investigations, including, but not limited to, monitoring workplace attendance, or work quality. However, recordings captured through standard surveillance may be utilized in cases of reasonable suspicion of policy or law violations, or as evidence in civil or legal proceedings. Information obtained in violation of this policy may not be used in disciplinary actions against University students or employees.

The University is committed to upholding ethical principles in the use of camera systems, including respect for individuals' privacy rights and the responsible use of surveillance technology.

Individuals and personnel with access to camera footage are expected to conduct themselves ethically and adhere to the highest standards of professional conduct. Ethical considerations shall be taken into account when accessing, viewing, and using camera footage for security monitoring and investigations, ensuring that actions are aligned with the University's Mission, Vision, Values, and principles; additionally, all use of camera and surveillance systems shall be in a manner consistent with other University policies, including but not limited to those relating to non-discrimination, sexual harassment, privacy, and freedom of expression. Personnel are encouraged to raise ethical concerns or questions regarding the use of camera systems with appropriate University authorities for review and resolution. Questions may be directed to the Office of Risk Management or Office of General Counsel.

V. Procedures/Implementation

A. Use of Camera Systems

1. Administrative Roles & Responsibilities

Risk Management: Responsible for overseeing the implementation, maintenance, and legal compliance of camera systems on campus.

Technology Services (IT): Responsible for the technical management, configuration, and security of camera systems, including access control and data protection measures.

University Police Department: Responsible for monitoring camera feeds, investigating security incidents, and ensuring compliance with campus security protocols.

2. Incident Response

Security concerns and potential violations of law or University policy detected through University camera systems shall be responded to by the appropriate authority, such as UPD or Housing & Residence Life staff. Surveillance system users shall cooperate with their counterparts in other divisions of the University to facilitate prompt and appropriate incident responses.

3. Use of Footage as Evidence

Footage that may be used as evidence in a disciplinary process, criminal investigation, or other similar context shall be excerpted and saved as a digital file maintained locally on a University data storage medium (*e.g.*, a hard drive or compact disk) pursuant to the typical policies and procedures of the monitoring University authority (*e.g.*, UPD). Such footage shall be kept either as long as is needed for the aforementioned proceeding to run to completion (including through the pendency of any appeals) or for one (1) year, whichever is longer.

4. Use in Compliance with Laws

The use of surveillance systems on campus is subject to applicable federal, state, and local laws and regulations, including but not limited to the following:

- Missouri Revised Statutes (RSMo) § 565.252: Addresses the unlawful use of electronic surveillance equipment.
- Missouri Sunshine Law (RSMo Chapter 610): Governs access to and privacy of public records, including video recordings.
- Family Educational Rights and Privacy Act (FERPA): Protects the privacy of student education records.
- Health Insurance Portability and Accountability Act (HIPAA): Protects health information in relevant areas of campus, such as medical centers.
- Missouri Privacy and Protection Acts: Regulates the collection, storage, and use of personal data.

5. Ethical Use – Confidentiality and Privacy

To ensure the ethical operation of University security cameras, all use of camera and surveillance systems shall be in accordance with the University's Mission, Vision, and Values, in addition to principles expressed in University policies and procedures. A corollary of this commitment is that all such use will be in conformity with federal (including but not limited to FERPA), state, and local laws, in addition to the letter and spirit of University policies. A decision to monitor a person or group's activity via camera systems shall never be based on characteristics of race, gender, ethnicity, sexual orientation, disability, or other protected classification unless the characteristic is part of a suspect's description in a specific offense. Moreover, monitoring shall never be used to harass, intimidate, discriminate against, or chill the protected speech of any individual or group.

The University recognizes the importance of respecting individuals' privacy rights in the use of camera systems on campus. Surveillance systems shall be deployed and operated in compliance with applicable privacy laws and regulations. Personnel handling camera footage are required to exercise discretion and judgment to minimize intrusions into individuals' privacy while conducting security monitoring and investigations.

Specifically with regard to confidentiality, all personnel with access to camera footage, either pursuant to a general grant of access privileges under the RBAC model or pursuant to a single access request, are required to treat the content of footage as confidential information and accept responsibility for its mishandling. Unauthorized sharing or disclosure of camera footage to individuals not authorized to access it is strictly prohibited.

6. Violations

Individuals and personnel responsible for managing camera systems shall be ultimately responsible for ensuring that the systems are only ever used in conformity with applicable legal requirements and University policies, both in the granting of access to footage and in the use and storage of recorded material.

Noncompliance with this policy may result in disciplinary action commensurate with the severity, scope, and circumstances of the violation. Such discipline may include revocation of access

privileges, suspension, termination, or such other measure deemed appropriate in light of the severity, scope, and circumstances of the violation.

B. Access to Camera Systems

Access to camera feeds is restricted to authorized personnel only. User access is based on a role-based access control (RBAC) model, with permissions tailored to specific user roles and responsibilities. The roles are as follows:

- Technology Services
- Risk Management
- University Police

Personnel with access to camera systems shall, prior to being granted those access privileges, complete a training program developed by the Director of Risk Management. This training will address confidentiality, privacy rights, legal compliance, and ethical considerations associated with camera usage.

The training will incorporate relevant federal compliance standards, including those under Title IV of the Higher Education Act, such as FERPA and institutional obligations related to student privacy.

Training will be periodically reviewed and updated to reflect changes in applicable law and University policy. Access will not be granted or renewed until the required training is completed.

If an individual who does not have access rights to a camera system under the RBAC model has a legitimate need to access such a system or footage saved from a camera system, then the individual should make a formal request of the appropriate custodian of the system or footage. Requests for footage access shall be reviewed and approved based on the requester's role, the purpose of the request, and compliance with applicable laws and regulations.

All personnel granted access to the University's camera systems acknowledge and consent to the following as a condition of access:

- **Monitoring of Activity:**
  - All actions performed within the camera system, including login activities, footage retrieval, and system access, are subject to logging and monitoring.
  - Activity logs will be reviewed periodically to ensure compliance with institutional policies and legal standards.
- **Review of Access:**
  - Any unauthorized or suspicious activity detected during routine monitoring may be investigated and may result in disciplinary action, including revocation of access privileges, suspension, or termination.
- **Acknowledgement of Consent:**
  - By accessing the camera system, users explicitly agree to these conditions and understand that their use of the system may be audited.

C. Security Camera Installation

Cameras may be installed in locations that support their intended purposes, provided they do not violate privacy expectations. Camera placement will be guided by the following principles:

- **Installation in Non-private Locations:** Cameras may be installed in restricted-access areas (e.g., labs) and public areas (*e.g*., walkways), where individuals do not have a reasonable expectation of privacy.
- **Monitoring Prohibited in Private Spaces:** Cameras will not be installed in private spaces such as bathrooms, locker rooms, or student bedrooms. When monitoring residential areas, camera views must prioritize privacy and exclude any areas where residents may have a reasonable expectation of privacy.
- **Visibility and Functionality:** All cameras must be visible and operational. The installation of hidden or non-functional "dummy" cameras is prohibited.
- **Audio Recording Permitted:** Cameras may include audio recording capabilities.

D. Department-Specific Camera Systems

Certain University departments may operate independent camera systems, such as those used for specialized purposes in athletics, research, or academic programs. These cameras are not part of the centralized security camera system and may operate under separate guidelines and software platforms. Irrespective of the department responsible for the particular camera system, certain principles will always apply.

First, departments are solely responsible for the operation, maintenance, and oversight of their respective camera systems. Any agreements with external software providers or third-party agencies for access to or management of these systems must comply with University policies, applicable laws, and data protection standards; additionally, any such agreements must pass through the University's normal contract approval process before being executed.

Second, department-specific cameras and camera systems shall not be integrated into the centralized University security system managed by the Risk Management, Technology Services, and UPD. Nevertheless, the University may require that recordings from department-specific camera systems be shared with these, or other subunits of the University as required for investigations. Furthermore, departments must request advance approval to add, remove, or relocate camera installations from Risk Management and Technology Services, and the University reserves the right to review department-specific camera usage to confirm compliance with broader University policies and regulations.

Finally, access to department-specific camera recordings shall be limited to authorized personnel within the department and appropriately authorized external members of the University and/or third parties. Such authorization shall be appropriate only if granted by the head of the department or the head's explicitly selected designee.

E. Evidence Management and Archiving

To ensure the integrity of investigations and the proper handling of digital evidence, the review and archiving of security camera footage shall be subject to oversight by the Vice President of Finance and Administration, responsible for policy compliance and governance.

Practical implementation and technical management of camera footage, including access control, system maintenance, and the fulfillment of approved review requests, may be delegated to designated personnel within Risk Management, Technology Services, or the University Police Department as appropriate.

All requests for camera footage review must be submitted to the oversight office, and both the purpose and scope of the request must be clearly specified. Approved requests will be logged, reviewed, and processed in accordance with applicable legal and policy standards, with the VPFA maintaining final accountability for compliance and recordkeeping.