FERRIS STATE UNIVERSITY

DIVISION OF ADMINISTRATION AND FINANCE

Security Camera Policy

Administration and Finance Business Policy

Policy Number: 2025:XX

This Policy pertains to the use of a video camera system (VCS) on campus to enhance the safety and security of students, faculty, staff, and visitors. The University recognizes that safeguarding the personal welfare of its students, staff and visitors is of paramount importance.

SCOPE AND APPLICABILITY

Ferris State University (FSU) operates a VCS for the purpose of creating a safer environment for all those who live, work and visit the campuses of FSU. The use of a VCS is intended to deter crime and assist in protecting the safety and property of the University community. In conjunction with the Security Access Control Policy, this policy addresses the University's safety and security needs while respecting and preserving individual privacy. This will enhance the student experience by leveraging technological capabilities, improving safety for students, faculty, and staff.

The purpose of this policy is to regulate the installation and appropriate use of video cameras. This policy applies to cameras installed or activated – permanently or on a temporary basis – specifically for purposes of enhancing campus safety and security.

The existence of this policy does not imply nor guarantee that video cameras will be monitored in real time, continuously or otherwise, nor that any department is going to observe and respond to an incident in progress.

POLICY

Efforts to promote campus safety and security by the installation of a VCS is primarily focused on, but not limited to, protection of individuals and property —including students, faculty, staff, and visitors. Video cameras may be used to monitor:

- University-owned and/or operated property and buildings;
- Cash-handling areas where money is exchanged, such as point-of-sale locations;
- Common areas and areas accessible to the public;
- Any other area deemed as necessary

Video camera systems generally cannot be installed in areas where there is a reasonable expectation of privacy. These areas include, but are not limited to:

- Restrooms
- Locker rooms
- Residential rooms

Recorded images shall not be made public, nor shall recorded images be released to, provided to, or otherwise made accessible to any person, party or entity inside or outside of the University, without the University's express permission, or as required by law.

No department or individual may install or operate a video camera or video camera system. Requests for cameras will be reviewed by the Campus Security Team. Only University-approved cameras are allowed on campus. If unapproved cameras are found, they will be confiscated.

Any abuse of this policy is subject to disciplinary action. This policy complies with all state and federal laws.

RESPONSIBILITIES

Location of and access to video cameras, the technology, and the strategy of the VCS will be managed by the Campus Security Team (CST) which includes (but not limited to):

- Department of Public Safety
- Facilities Management
- Information Technology Department
- Safety, Health, Environment, and Risk Management Office (SHERM)
- Purchasing
- Student Affairs - including Housing
- Academic Affairs

- Overarching guidance of the Vice President of Administration & Finance

The CST may grant exceptions to this policy. Exceptions, including their rationale, must be documented in writing. Cameras used for Athletic purposes, Capital Construction projects, and Osprey observation are excluded from this policy.

Access to the VCS to view video will be granted to a limited number of staff members (VCS users) as approved by the CST (based on requests from Vice Presidents), based on a business case need. Access to live and recorded video footage is restricted to authorized personnel such as the Department of Public Safety and designated administrative staff. Video footage will be monitored and reviewed as necessary.

Camera video is stored in a secure, centralized VCS for a minimum of thirty (30) days, unless exported and retained as part of a criminal investigation or court proceedings (criminal or civil), or other bona fide uses as approved by the Director of Public Safety or their designee.

The Chief Information Officer or their designee is responsible for the testing and coordination of the support and maintenance of the VCS. This includes maintaining a master list of all cameras. The Chief Information Officer is also responsible for the installation, support, maintenance, replacement, and decommissioning of hardware and software components that comprise the University VCS with the assistance of the CST noted above.

All requests to obtain recorded images must be submitted via the Freedom of Information Act (FOIA) to the FSU General Counsel's office.

VCS operators are trained in the technical, legal, and ethical parameters of appropriate video camera use. All operators will be required to sign a confidentiality statement noting that they have been properly trained.

CORRESPONDING POLICIES/PROCEDURES

A. Video Camera System Procedures
B. Security Access Control Policy
C. Security Access Control Procedures

CONTACTS

For more information, please contact the following departments:

- Department of Public Safety
- Facilities Management
- Information Technology

Amanda Matheson
Vice President for Administration & Finance