FERRIS STATE UNIVERSITY

DIVISION OF ADMINISTRATION AND FINANCE

Security Camera Procedure

Administration and Finance Business Procedures

Procedure Date: 2025:XX

PROCEDURE

Ferris State University (FSU) has created the Campus Security Team (CST), which is responsible for centralizing the operation, maintenance, and administration of the video camera system (VCS). These procedures will be continuously modified to accommodate the growth of this effort.

NEW CONSTRUCTION & MAJOR REMODELS

Facilities Management, with support from professional consultants, has developed a campus camera standard that will apply to all new construction and major remodels. Facilities Management understands that the building's needs may exceed the standard, and it will collaborate with the building occupants to include any additional cameras necessary to provide the desired coverage of the building. The cost of the cameras, data cables, license, and installation will be included in the construction costs of the project.

REQUESTS FOR NEW CAMERA(S) IN EXISTING FACILITIES

Departments may submit a request for a new camera with the Vice President's approval. The CST will review the request and either approve or deny it based on the attributes noted below. If approved, the CST will cover the cost of installation and ongoing operation for the additional

camera. If the request is denied, the department may not, under any circumstances, install a video camera or a video camera system.

ATTRIBUTES REQUIRED FOR A NEW CAMERA REQUEST

Users wishing to request a new camera(s) will need to provide the location requested, the number of camera(s), and an assessment of the security need.

The request will be managed via a form that includes (but is not limited to) the following characteristics:

- Risk Level Assessment
- Cash Handling
- High Traffic Areas
- Existing Camera Locations and Coverage

REQUESTING ACCESS TO VIEW SECURITY CAMERAS

Departments, with the Dean's, VP's, or President's approval, may submit requests for access to live video feeds from one or more cameras for legitimate security purposes. The CST will review the request and either approve or deny it. If approved, Information Technology Services (ITS) will collaborate with the users who will be viewing the camera footage and assign them access as Security Camera System Viewers. This will be managed through a request form that identifies the person/department and the justification for the request.

SECURITY CAMERA SYSTEM VIEWERS

Security Camera System Viewers (SCSV) are trained staff members who have access to live camera feeds and have been assigned responsibility by the University. Before granting these individuals access to any security cameras, the University will train them in the technical, legal, and ethical parameters of appropriate camera use. The VCS will maintain an up-to-date list of authorized SCSVs with access to live camera feeds.

SCSVs are responsible for protecting the privacy of personal information that live cameras may capture under their control. SCSVs are not to use a phone or any other recording device to capture live video or share live video with anyone not permitted to see said video.

SECURITY CAMERA SYSTEM VIEWERS (With Playback Functionality)

Security Camera System Viewers (with playback functionality) are trained staff members who have access to live camera feeds, playback functionality, and have been assigned this responsibility by the University. Before granting these individuals access to any security cameras, the University will train them in the technical, legal, and ethical parameters of appropriate camera use. The VCS will maintain an up-to-date list of authorized Security Camera System Viewers (with playback functionality) with access to live camera feeds.

SCSVs are responsible for protecting the privacy of personal information that live cameras may capture under their control. SCSVs (with playback functionality) are not to use a phone or any other recording device to capture live video or share live video with anyone not permitted to see said video.

SECURITY CAMERA SYSTEM OPERATOR

Security Camera System Operators (SCSO) are granted access to any security cameras, these individuals will be trained in the technical, legal, and ethical parameters of appropriate camera use. The VCS will maintain an up-to-date list of authorized SCSOs who have access to the system and any live or recorded images. Access to viewing, copying, duplicating, and/or

retransmitting live, recorded video or still images will be limited to the Department of Public Safety (DPS).

SCSOs are responsible for protecting the privacy of personal information that live cameras may capture under their control. SCSOs are not to use a phone or any other recording device to capture live video or share live video with anyone not permitted to see said video.

RECORDINGS

Images recorded by video camera systems are considered sensitive information that must be protected from unauthorized access, modifications, duplications, or destruction. The recorded video generated by university video cameras is to be kept in a secure location.

Recorded video may be released when it is related to any criminal investigation, civil suit, subpoena, court order, arrest, or to aid in a disciplinary proceeding. Recorded videos that need to be retained as part of a civil or criminal investigation may be downloaded and retained by law enforcement personnel. Internal requests to release recorded video are to be authorized by the Director of Public Safety, FSU General Counsel, or their designee(s). This would include FOIA requests that FSU General Counsel receives.

All recordings are overwritten every 30 days unless there is a demonstrated security need, ongoing investigation, court order, or other bona fide use as approved by the Director of Public Safety or their designee.

MONITORING

University video cameras may not be continuously monitored under normal operating conditions, but may be observed for legitimate safety and security purposes. These purposes include, but are not limited to, the following: high-risk areas, restricted access locations, responses to alarms, special events, and specific investigations authorized by the Director of Public Safety or their designee(s).

Any person who tampers with or destroys video security equipment will be subject to criminal prosecution and/or campus disciplinary processes.

AUDITING CAMERA ACCESS

The CST will review all VCS users on a routine basis, at least twice per year. Users who are no longer employed or who no longer need to access the VCS will be removed. Users who were granted access but have not used that access consistently may also be removed.

MAINTENANCE

The VCS will be supported by a centrally funded budget and collectively supported by DPS, Facilities Management, and Information Technology Services. If needed, ITS will replace failed cameras with the support of Facilities. ITS will maintain the servers used to store the video, along with the aid of the selected maintenance and support vendor.

CORRESPONDING POLICIES & PROCEDURES

A. Video Camera System Policy 2025:XX
B. Security Access Control Policy 2025:XX
C. Security Access Control Procedures
D. Link to the form needed to request access

CONTACTS

For more information, please contact the following departments:

- Department of Public Safety
- Facilities Management
- Information Technology

Amanda Matheson
Vice President of Administration & Finance