FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Video Surveillance System (VSS) #520.025

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
August 1 2024	October 1, 2024	Facilities Management FIU Police Department Office of General Counsel

POLICY STATEMENT

This policy applies to all FIU Students, Faculty, Staff and POI's in the University that may interact or have access to the Video Surveillance System (VSS). The policy strives for safety, security and privacy for all occupants and properties. The safety and security of the University's facilities and assets is a shared responsibility of all members of the University community.

REASON FOR POLICY

This policy seeks to achieve the following objectives:

1. Define the scope of the VSS regarding who the policy applies to and what locations are covered.
2. Identify roles and responsibilities of the University stakeholders detailing use of the VSS, and the dissemination of surveillance records.
3. Define the access & approval process.
4. Discuss dissemination of information about the VSS.

SCOPE

This policy applies to all FIU Students, Faculty, Staff and POI's. This policy applies to all FIU VSS located at the Modesto Maidique Campus (MMC), Engineering Center (EC), and Biscayne Bay Campus (BBC), Wolfsonian and FIU DC.

For off campus facilities and sites that are either owned by FIU or leased and that operate an independent VSS, the University requires a minimum standard for the operation of the VSS to include the following:

- Communication with Human Resources (HR) either via an automated or manual feed to ensure that the processing of termination and transfers for employees and POI's that have access to the VSS are handled in a timely manner.

- Ensure that FIUPD has direct remote access 24x7 to the VSS and that physical access to the system is granted when requested.
- Ensure that surveillance footage retention is 30 days or greater.
- Ensure that cameras procured and installed on the FIU network are compliant with the NDAA Act of 2019 section 884 requirements.
- Any purchase of a VSS must be screened and approved by the Facilities IT Director.
- Ensure that the cameras and storage attached to the FIU network are secured by working directly with DoIT to ensure proper network security.
- Ensure that download of video is restricted and that only with authorization of the Office of General Counsel can the footage be released to any third party or other members of the FIU community.

Any external third parties or government agencies requiring access to the VSS would need to coordinate and receive written approval from Office of General Counsel.

University departments and third-party vendors doing business on campus are NOT allowed to install their own VSS unless approved by FIUPD and the Office of General Counsel as an exception to this policy. The current exception to this policy includes the following department(s) that have been authorized to install their own VSS.

1. University Operations & Safety Parking and Transportation Department
   - LPR System
   - Garage Roof Analytics Project
   - Parking Enforcement and Count Availability

This policy also does not apply to the applications listed below:

- Cameras used covertly by law enforcement for criminal surveillance.
- Remote monitoring of facilities construction to ascertain project progress.
- Campus public relations initiatives.
- Videotaping of athletic events for post-game reviews.
-

DEFINITIONS	
TERM	**DEFINITIONS**
Video Management Software (VMS)	Software used by FIU for camera surveillance and footage review/retrieval.
Video Surveillance System (VSS)	Is the entire system, comprised of IP cameras and server storage used for the purpose of security surveillance of Facilities and University Assets.

ROLES AND RESPONSIBILITIES

University Stakeholders:

Facilities Management Information Technology (FMDIT) – has responsibility for the entire VSS from the perspective of being the technical custodian of the system. FMDIT does not use the VSS for any purpose other than to maintain the system.

FIU Police Department (FIUPD) – agency that uses the VSS for daily operations. FIUPD uses the cameras for investigations, real time monitoring and retrieval of archival footage. Provides guidance for the dissemination of footage related to criminal matters.

University Departments – departments use the VSS for operational business needs but have limited access to only the cameras in their area of responsibility. Departments do not have the ability to download or disseminate footage unless authorized as an exception to policy.

General Counsel – Does not use the VSS. Provides guidance on public requests, subpoenas and any dissemination of footage requested by a third party.

Risk Management – Does not use the VSS. provides guidance on the dissemination of footage on any personal injury cases that may arise.

Human Resources – Does not use the VSS. provides guidance on the dissemination of footage or usage of cameras for HR related matters.

Emergency Operations Center (EOC) – has access to VSS for use in the event of an emergency which may require the monitoring of the cameras.

Division of Information Technology (DoIT) – has limited access to the VSS related to areas in their area of responsibility. DoIT, actively manages and provides guidance for the network security of the VSS. DoIT is responsible for the FIU network infrastructure between the camera and the server. DoIT is also responsible for the security policies in place that provide secured access to the VSS both on campus and remote.

ACCESS & APPROVAL PROCESS

Students do NOT have access to the VSS. Only employees are allowed access, and POI's are granted access to the surveillance system based on an approved business need.

A prior written request is required for any access. In the written request FMDIT requires the scope of access, Panther ID, Name, level of access, and duration if applicable. Depending on the nature of the request FMDIT will request approval from the above University stakeholders.

For access to all surveillance cameras at the University, FMDIT requires written authorization from FIUPD and the Office of General Counsel.

For departments that have a business need to access only the cameras in the areas they manage, access is provided to the department manager that requested and paid for the cameras after it has been approved by one of the University stakeholders. If they require any additional staff that need access, FMDIT requires written authorization from that department manager detailing the scope of the access, Panther ID, Name, and duration.

For temporary access, FMDIT evaluates the nature of the request and forwards that to one of the University stakeholders listed above (i.e. General Counsel, Law Enforcement, etc.). FMDIT then requires a written authorization from the stakeholder detailing the type of access and the duration.

DISSEMENATION OF INFORMATION RELATED TO THE VSS

No FIU employee or POI is allowed to disseminate any information regarding the operational components (i.e. camera views, camera locations, etc.) of the VSS to anyone inside or outside the University or to a third-party law enforcement agency without written authorization by the Office of General Counsel. This does not prohibit FIUPD from dissemination of information about the VSS to third party law enforcement agencies regarding an active investigation.

RELATED RESOURCES

N/A

CONTACTS

Facilities Management
Florida International University
11200 S.W. Eighth Street, CSC 220
Miami, Florida 33199
Telephone: (305) 348-4001

HISTORY

Initial Effective Date: August 1, 2024
Review Dates (review performed, no updates): N/A
Revision Dates (updates made to document): October 1, 2024