	Florida Tech Department of Security Written Directive System	10:01
	VIDEO MANAGEMENT SYSTEM (VMS)	
	Effective Date: May 26, 2020	**Approved by:** **T. Dwayne McCay, President**

NOTE: This written directive is for the internal governance of Florida Tech Department of Security and is not intended and should not be interpreted to establish a higher standard of care in any civil or criminal action than would otherwise be applicable under existing law.

POLICY: VMS, Video Surveillance

Florida Institute of Technology is committed to enhancing the safety of members of the University community. Toward that end, it is the policy of the University to utilize a Video Management System, herein referred to as VMS, to enhance personal safety, help deter crime, collect information and evidence of actual or potential criminal activity, and protect property. The use of VMS will be conducted in a manner consistent with the values of the University and in compliance with all existing University policies and all applicable state and federal laws. The VMS and equipment shall operate under the authority of the Director of Security.

PURPOSE:

The purpose of this policy is to regulate the use of VMS cameras used to monitor persons and places within Florida Institute of Technology.

PROCEDURES

All video monitoring will be conducted in a professional, ethical and legal manner. Personnel involved in the use of video equipment will be appropriately trained and supervised in the responsible use of this technology. Any information obtained through video recording and/or monitoring may be used for public safety and law enforcement purposes and for compliance with Florida Institute of Technology policy. Information obtained through video recording/monitoring will only be released when authorized by the Director of Security.

Video monitoring of areas for public safety at Florida Institute of Technology is limited to locations that do not violate reasonable expectations of privacy as defined by law.

RESPONSIBLITIES:

All operators and supervisors involved in the use of video monitoring will perform their duties in accordance with policy developed by the Department of Security and Florida Institute of Technology. All members of the Department of Security shall be considered to be VMS operators.

1. Personnel are prohibited from using or disseminating any of the information acquired from the video equipment except for official purposes. All information and/or observations made in the use of VMS equipment are considered confidential and can only

be used for official University and law enforcement business upon approval of the Director of Security.

2. Any copying, "burning", printing, and/or e-mailing of VMS information for other than law enforcement purposes shall only be done with the approval of the Director of Security, University President and the University Attorney.
3. VMS monitoring shall NOT be used for the following;
    a. Random and/or specific monitoring or targeting of individuals based to any degree upon the race, gender, ethnicity, national origin or stereotyping of any form.
    b. Peering into buildings, private office space, restroom facilities, locker rooms or other areas where there is an expectation of privacy, except for legitimate campus public safety purposes, such as a criminal investigation.
    c. Audio monitoring/recording
4. Selection of locations for the installation of VMS cameras will be determined by members of this department based upon a data-driven need at a specific location. Consideration should be given to crime trends, public perception and the potential for criminal activity. Any decision will be made in consultation with the Vice President of Operations or designee to ensure planned technologies are appropriate/available as proposed.
5. Recorded events are stored temporarily until overwritten on the systems hard drive as part of its Digital Video Recording (DVR), unless retained as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved. The storage capacity of each camera within the overall system is determined by multiple factors, including but not limited to, the number of images captured, the quality of images captured, etc... As a general rule, video recordings are retained on the Digital Video Recorder (DVR) associated with the VMS Camera for a minimum of ten (10) calendar days after which time they will be recorded over.
6. Should monitoring reveal activity that violates laws or policies, an investigation will be initiated. The viewer shall complete an incident report to include a statement depicting what was observed from the employee monitoring the VMS camera. The report will be forwarded to the Director of Security who will initiate an investigation and if necessary, notify local police.
7. Concerned citizens, victims, suspects, news media and other non-authorized persons shall NOT be allowed access to monitoring or digital recordings unless approved by the Director of Security.
8. Under no circumstances shall anyone, except professionally trained technicians, the Director of Security or qualified members of Information Technology, attempt to service, repair, or tamper with any of the video surveillance equipment.
9. The Department of Security is the office authorized to oversee and coordinate the use of VMS monitoring for safety and security purposes at Florida Institute of Technology. All university offices and units using the VMS are responsible for implementing this policy in their respective operations.
10. Video capture software is expressly prohibited on computers with access to University surveillance cameras.

11. Requests from University entities to release information obtained through surveillance cameras must be submitted to and approved by the Director of Security, the Vice President of Operations or President prior to release.
12. All requests from sources external to the University to release information obtained through surveillance cameras must be approved by the University Attorney, Vice President of Operations or President.
13. Surveillance cameras utilized for any criminal investigations are subject to appropriate State and Federal laws and are excluded from this policy.
14. In order to provide proper maintenance Network Security and the IT Network Security Leadership shall have complete system access.
15. At least annually, the Director of Security or designee shall evaluate the current locations and technical deployments of all cameras within the University's VMS.
    - This review is intended to make recommendations regarding additional deployments as well as modifications to existing cameras with appropriate deference given to incident reported to and investigated by this department.
    - This review shall be documented in a written report to the Director of Security with geographic responsibility and completed annually by January 10th of each calendar year.