

**UCF Video Camera Standards**

Current as of:

April, 2021

# LETTER OF PROMULGATION

The Department of Security (DS) is the designated security program for the University of Central Florida (UCF) with the authority, through its Director, to implement UCF’s physical security on behalf of the jurisdiction. The DS’s authorities and responsibilities are established in, and executed in accordance with, applicable federal and state laws, Florida statutes, and University regulations and policies.

The Department of Security is responsible for managing the physical security systems of UCF campuses.

The Director of Security Management is responsible for developing, implementing, and managing institution-wide physical security best practice systems, plans, policies, and procedures. This position serves the university community by assisting campus administrators (senior leadership, staff and faculty) with matters involving physical security. The Director of Security Management is the designated contact, who will act as the university’s liaison to external vendors and partners in the area of security.

For this document, the purpose of the UCF Video Camera Standards is to provide the framework for the management and appropriate use of the video management system. It clarifies responsibilities and procedures for accessing, using, and modifying any part of the UCF video cameras or video management system.

This is a dynamic document that is ever-changing. A standard review process accompanied by rigorous testing and review, will ensure that these standards do not become another "manual on the shelf."

Approved by:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Carl Metzger, Associate Vice President and Chief of Police Date

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Gerald Hector, Senior Vice President of Administration and Finance Date

Table of Contents

[LETTER OF PROMULGATION 2](#_Toc38611420)

[Chapter 1: General 5](#_Toc38611421)

[Chapter 2: Responsibilities 7](#_Toc38611425)

[Chapter 3: Violations and Sanctions 8](#_Toc38611441)

[Chapter 4: Installation 9](#_Toc38611449)

[Chapter 5: Maintenance 11](#_Toc38611450)

[Chapter 6: Video Management System 12](#_Toc38611451)

[Chapter 7: Video Management System Access 13](#_Toc38611452)

[Chapter 8: Training 16](#_Toc38611462)

[Chapter 9: Operation 17](#_Toc38611463)

[Chapter 10: Multipurpose Video Cameras 20](#_Toc38611472)

[Appendix I: Acronyms, References & Definitions 21](#_Toc38611478)

These standards are maintained by the University of Central Florida’s Department of Security. Any concerns or questions can be forwarded to:

Department of Security

Email: DS@ucf.edu

**Departments Responsible for this plan:**

* Department of Security

**Supersedes:**

* First edition (February 2018)

**Pages:**

* 22

**Notes:**

# Chapter 1: General

## Purpose

* + 1. To ensure the protection of individuals, property, and privacy rights in accordance with the University’s core values and federal and state laws, this standard is adopted to formalize procedures for the handling, viewing, retention, dissemination, and destruction of recorded images. The purpose of this standard is to regulate the use of University video cameras and the video management system installed and operated in all UCF facilities and properties.

## Principles

* + 1. UCF is committed to the use of reasonable measures to mitigate potential threats and improve solvability factors related to crime on our campus. A critical component that assists in this endeavor is the use of video cameras and other image capture tools.
		2. UCF’s Department of Security reserves the right to place video cameras where necessary and appropriate. The Department of Security respects the right to privacy of the University community (Section 9.6).
		3. Video cameras provide a visual deterrent to crime, assist with overall security measures, and increase the potential identification and apprehension of person(s) who violate University regulations or policies and/or commit criminal acts. Video cameras are not a guarantee of safety; however, they do serve as deterrents and can alert the UCF Police Department and Department of Security to potential danger. The primary use of video cameras is to record images for future identification of individuals and activity in the event of violations of law or University regulations or policies.
		4. University video cameras are not monitored continuously under normal operating conditions, but may be monitored for legitimate safety and security purposes that include, but are not limited to, the following: life safety situations, high risk areas, restricted access areas/locations, in response to an alarm, special events, and active criminal activity.
		5. UCF also utilizes video cameras to support education, research, health care, and the protection of critical infrastructure and key resources. These video cameras must also adhere to these standards.
		6. All recording or monitoring of activities by University video cameras shall be conducted in a professional, ethical, and legal manner consistent with University regulations and policies, state and federal laws, and shall not be based on the subjects’ personal characteristics, including age, color, disability, gender, national origin, race, religion, sexual orientation, or other protected characteristics.
		7. The purchase and installation of any video camera system (hardware, software, or related equipment) whether it’s connected to the network or an isolated system is required to be reviewed and approved by the Department of Security. This includes video cameras purchased with department funds, grants, or any other UCF funding source.

## Scope

* + 1. All members of the University community (students, faculty, staff, and guests), those doing business with or at the University, and those on University controlled property must fully comply with these standards.
		2. These standards do not apply to use of video cameras used for the following:
			1. Video cameras used for journalistic purposes;
			2. Video cameras used for broadcasting public events or performances;
			3. Video cameras used for web or video conferencing, marketing and recruitment;
			4. Video cameras on mobile devices such as smartphones, tablets, and laptops; or
			5. UCF Police body cameras or video cameras located in UCF Police Department patrol vehicles.

# Chapter 2: Responsibilities

## Department of Security Responsibilities

## The Department of Security is responsible for:

## the realization, assimilation, and enforcement of these standards;

## reviewing and approving or denying any requested exceptions to these standards;

## proposing appropriate changes to these standards to the Associate Vice President and Chief of Police, as needed;

## reviewing and approving or denying all proposals for video camera equipment;

## advising departments on appropriate applications of camera technologies and for providing assistance to departments preparing for the purchase and installation of camera systems;

## monitoring developments in federal and state laws, current trends in technology, and continuing to implement best practices;

## reviewing and approving proposals and recommendations for video camera installations, as well as reviewing specific video camera types and locations to ensure the best view and image quality is captured;

## maintaining and testing video camera hardware and software; and

## reviewing any complaints regarding the operation of video cameras and determine whether these standards are being followed.

## Operator Responsibilities

## Operators are responsible for:

## performing his or her duties in accordance with these standards, and

## accessing live video or recorded images only to the extent permitted by these standards.

## notifying the Department of Security if he or she believes a video camera is not functioning properly

# Chapter 3: Violations and Sanctions

## Sanctions

## Failure to comply with these standards could result in one or more of the following, but not limited to:

## Loss of video camera access privileges;

## Institutional sanctions up to and including termination of employment; and

## Legal action.

## Any person who tampers with, damages, or destroys video camera equipment will be subject to criminal proceedings and/or disciplinary action.

## Unauthorized, unethical or illegal use or installation of a video camera in violation of these standards may subject an employee or student to disciplinary action and/or criminal proceedings.

## Reporting

* + 1. Concerns about possible violations of these standards related to inappropriate use of video cameras or the video management system should be directed to the Department of Security.

# Chapter 4: Installation

* 1. Installation, Relocation, and Removal
		1. Requests for installation, relocation, and/or removal of video cameras in/on University property must be coordinated with and approved by the Department of Security.
			1. Installations of video cameras in/on new building construction and/or building renovations must be coordinated with Department of Security and Facilities Planning and Construction.
				1. Renovations exceeding 50% of a building’s space requires the entire renovation meets current Department of Security recommendations for video camera installations.

Space percentage is determined by Facilities Planning and Construction

* 1. Processes
		1. Requests for installations of new video camera(s)in/on existing buildings must be submitted to the Department of Security using the *UCF Camera Installation Request* form located at <http://police.ucf.edu/securitycameras>.
		2. Requests for modifications of video camera(s), including, but not limited to, relocating, repositioning, upgrading, and/or removal must be submitted to the Department of Security using the *UCF Camera Maintenance Request* form located at <http://police.ucf.edu/securitycameras>.
		3. The Department of Security will review and approve or deny the request based on the business justification provided in conjunction with a site security survey.
		4. The Director of Security will review and has final approval for all proposals. Appeals will be submitted in writing to the Department of Security and will be reviewed by the Associate Vice President and Chief of Police for final decision.
		5. The department or college requesting video cameras will be responsible for the initial cost of the video camera, storage hardware and related installation costs of hardware and supporting network as well as initial software licensing fees. The Department of Security will help to identify additional costs associated with the video camera project, upgrade, or installation.
	2. Departments requesting grant funding to add and/or alter any new or existing video camera and/or systems must obtain prior approval from the Department of Security.
		1. Any grant or technology fee proposal for additional video camera equipment or modification to existing camera equipment, regardless of its intended purpose, must be compliant with all associated standards including UCF Video Camera Standards.
	3. All new installations of video cameras scheduled after the effective date of these standards must be in compliance with the terms and conditions of these standards.

* 1. The Department of Security will oversee the physical installation of all pre-approved video camera hardware.
	2. The installation of "dummy" or false video cameras that do not operate is prohibited.
	3. The department or college in possession of video cameras that are no longer functional must remove all devices and related hardware at their own expense and in accordance with UCF IT Telecommunications and Facilities Planning and Construction standards.
	4. Video camera equipment, devices, or systems installed without appropriate authorization after publication of these standards will be immediately disabled upon notice and if not reauthorized under these standards, will be removed at the expense of the department found to be responsible.

# Chapter 5: Maintenance

* 1. All camera repairs and replacements must be coordinated through and authorized by the Department of Security.

5.2 Any maintenance, servicing, or repair performed on a video camera must be done so by a UCF-approved vendor or contractor. At no time shall any UCF personnel perform physical maintenance on video cameras unless authorized to do so by the Department of Security.

# Chapter 6: Video Management System

* 1. Video camera systems are centrally managed by UCF Department of Security.
	2. Milestone Xprotect Corporate is the only approved video management system used to access live video and recorded images. All new University video camera hardware must operate on the Milestone Xprotect Corporate Video Management System (VMS).
	3. Milestone Xprotect Management Client is the software used to manage the administrative controls and overall configuration for the Milestone Xprotect Corporate VMS.
		1. The Department of Security will be the administrators of the Milestone Xprotect Management Client.
	4. Milestone Xprotect Smart Client is the only UCF-approved video management software used to access live video and recorded images. Milestone Xprotect Smart Client access will be controlled by the Department of Security.
	5. Video camera systems that were installed prior to the effective date of these standards shall be immediately configured to provide management and viewing access to the DS and transitioned into Milestone Xprotect Corporate within three (3) years of the date of adoption. Generally, the department will be responsible for any costs associated with transitioning legacy systems to be compliant with these standards.

# Chapter 7: Video Management System Access

1.
2.
3.
4.
5.
6.

## University Video Camera Access

* + 1. Accessing a physical video camera using the video camera’s internet protocol (IP) address or by any other means (other than by using the approved video management system) is only permitted to those authorized by the Department of Security.
		2. The alteration of any hardware, software, or network feature of a University camera is only permitted to those authorized by the Department of Security. Departments interested in altering video camera features are encouraged to consult with the Department of Security to determine appropriateness.
		3. The alteration of the physical network infrastructure connected to any University camera is only permitted by UCF IT Telecommunications personnel in partnership with the Department of Security.

## Milestone Xprotect Management Client

* + 1. The Milestone Xprotect Management Client is the software used to manage the administrative controls and overall configuration for the Milestone Xprotect Corporate video management system.
		2. Access to the Milestone Xprotect Management Client is only permitted to Department of Security personnel.
		3. Approved personnel within UCF IT may have access to the physical and virtual servers hosting the Milestone Xprotect Management Client(s). However, accessing the Milestone Xprotect Management Client by UCF IT or any personnel outside of Department of Security without the Director of Security’s approval is strictly prohibited.

## Milestone Xprotect Smart Client

* + 1. The Milestone Xprotect Smart Client is the software used by Operators to view live video and recorded images from video cameras.
		2. Anyone requesting access to Milestone Xprotect Smart Client must obtain authorization from the Department of Security. Requests must be made using the *Milestone Access Request* form located at <http://police.ucf.edu/security>.
		3. Only personnel approved and trained in the use of the video management system are permitted to operate the Milestone Xprotect Smart Client. Failure to comply may result in punitive actions by UCF.
		4. Operators of the Milestone Xprotect Smart Client are prohibited from:
			1. Sharing their password and/or login credentials to anyone at any time. Operators will report to the Department of Security as soon as possible and reset their NID password if they believe their password has been compromised or used without their permission.
			2. Viewing the interior of residential rooms, offices, or locations with a reasonable expectation of privacy, through windows, doors, or other means. Video cameras shall not be directed at the windows of any privately-owned residence.
			3. Duplicating images or permitting access to others except as specifically permitted by these standards.
			4. Viewing, recording, accessing, or otherwise using the video management system in any manner that is inconsistent with these standards and/or outside the scope of the usage approved by the DS.
		5. The information below identifies the different Milestone Xprotect Smart Client access levels for Administrators and End Users:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Security Level** | **Export (download footage)** | **Playback/Recorded Images** | **Live Camera Feeds** | **Management Client/System Administration** | **ALL UCF Cameras** | **Pre-Determined Access** |
| **1** | **X** | **X** | **X** | **X** | **X** | Security |
| **2** | **X** | **X** | **X** |  | **X** | PD Detectives |
| **3** |  | **X** | **X** |  | **X** | PD Dispatch | Emergency Management  |
| **4** |  |  | **X** |  |  | Parking Services |
| **5** |  | **X** | **X** |  |  | Department Level Playback |
| **6** |  |  | **X** |  |  | Department Level Live |

* + 1. Security Level 1 or administrative access is permitted only to the Department of Security (DS) personnel. Access is assigned by the Director of Security.
		2. Requests for public records release, related to recorded images and video, must be immediately directed to the Department of Security. End users must not release recorded images or video in response to a public records request.
		3. The copying, duplicating, or exporting of live video or recorded images shall be limited to the University Criminal Investigations Division and Department of Security personnel. Authorized users are approved by the Associate Vice President and Chief of Police or the Director of Security.

			1. Requests to export or download camera footage must be submitted to the Department of Security using the *Camera Footage Request* form located at <http://police.ucf.edu/security>.
		4. Security Level 3 or access to all University live video & recorded images shall be limited to University Police Department dispatch and investigators, Department of Emergency Management personnel, and Department of Security personnel. Authorized users are approved by the Associate Vice President and Chief of Police and the Director of Security.
		5. UCF employees may request access to view live video, located within their respective departments, by submitting the *Milestone Access Request* form located at <http://police.ucf.edu/security>.

			1. Access requests will be reviewed and accepted or rejected by the Director of Security based on the business justification provided.
		6. For access permissions to License Plate Recognition devices, see section 10.4.

# Chapter 8: Training

* 1. Those who have been approved to use the Milestone Xprotect Smart Client will be trained in the requirements of these standards and the technical and ethical parameters of appropriate video camera use. Training will be led by Department of Security personnel.
	2. Training for the Operators will be scheduled and conducted once the *Milestone Access Request* formis submitted to and approved by the Department of Security. The form is located at <http://police.ucf.edu/security>.
	3. Each Milestone Xprotect Smart Client Operator must complete the Milestone Xprotect Smart Client End-User Training, provided by Department of Security.
	4. Access will not be granted to the Operator until he or she has completed the required training courses stipulated in section 8.3.
	5. Operators of the video management system will receive a copy of these standards and provide written acknowledgement they have read and understand its contents and will perform their duties in accordance with these standards. Operators are responsible for being aware of all changes or revisions to the UCF Video Camera Standards. All changes or revisions will be posted to <http://police.ucf.edu/security>.

# Chapter 9: Operation

1.
2.

## Audio

* + 1. Audio recordings shall be prohibited unless specifically requested by a department and authorized by the DS.
		2. Multipurpose video cameras, as referenced in Chapter 10, may record audio once authorized by the Department of Security.
		3. Signage must be posted in UCF spaces where there is audio recording of faculty, staff, students, and/or guests.
			1. Signage will state at a minimum:

**THIS AREA MAY BE SUBJECT TO AUDIO RECORDING AND VIDEO SURVEILLANCE UNDER THE DIRECTION OF THE UNIVERSITY OF CENTRAL FLORIDA**

## Covert Video

* + 1. The use of covert video may only be used in special and unique circumstances and must be approved by the Associate Vice President and Chief of Police and Director of Security.

## Protection & Retention of Recorded Images & Audio

* + 1. Alteration
			1. No attempt shall be made to alter any part of recorded images.
			2. The use of personal recording devices and third-party software (including but not limited to: cell phones, camcorders, Skype and tablets) to record live video and/or recorded images from our video management system is strictly prohibited.
		2. Recorded Images & Audio Storage
			1. Recorded images and audio shall not be stored by individual departments unless authorized by the Department of Security.
			2. Recorded images and audio shall be stored in a secure location with access limited to only authorized personnel, designated by the Department of Security in conjunction with UCF IT.
			3. Recorded images will be stored for a minimum period of 30 days and thereafter may be erased, if not otherwise required for any related investigation, claim, or other University requirement authorized by the Department of Security.
			4. A request must be submitted to the Department of Security for video cameras to retain recordings for periods longer than 30 days.

## Release of Recorded Images

* + 1. Recorded images are exempt from public release per Florida statutes 1004.0962 and 119.071(3)(a). Waivers of the exemptions may only be executed by the Associate Vice President and Chief of Police or Director of Security.
		2. Unauthorized release of recorded images is strictly prohibited and could result in disciplinary action as referenced in section 3.1.
		3. UCF personnel and departmental requests for recorded images must be submitted to the DS who will coordinate with UCF Police Department. No department personnel, including the dean, director, or designated executive authority, can authorize the release of recorded images.
		4. Recorded images under active law enforcement investigation, audit or compliance investigations, or other UCF investigations will not be released to any party without approval from the investigating authority.

## Audit

* + 1. For the purposes of investigating misuse or disuse of the video management system, electronic audit logs may be reviewed by the Department of Security of all instances of access to or use of video cameras and video management system. The log shall include the date and identification of the person(s)to whom access was granted.

## Expectation of Privacy

* + 1. Operators of the Milestone Xprotect Smart Client are prohibited from viewing the interior of residential rooms, offices, or locations with a reasonable expectation of privacy, through windows, doors, or other means.
		2. Where video cameras are permitted in private areas, they will, to the maximum extent possible, be used narrowly to protect persons, money, property, documents, supplies, equipment, or pharmaceuticals from theft, destruction, or tampering.
		3. Departments and colleges shall use the video management system for reasons directly related to campus safety and security, including investigating crimes and policy violations or monitoring unstaffed spaces. Using the video management system in the following ways is prohibited: to serve personal interests or satisfy personal curiosity by monitoring employee and student movements, associations, and activities; to interfere with an individual’s reasonable expectation of privacy; or for purposes related to the evaluation of employee job performance, including as a means to track employee attendance. Requests to use the video management system in ways other than monitoring and/or investigating issues directly related to safety and security must be approved by the Associate Vice President and Chief of Police or designee.

# Chapter 10: Multipurpose Video Cameras

1.

## Student Conduct Video Cameras

* + 1. The Office of Students Rights & Responsibilities (OSRR) may utilize video cameras, within the guidelines of these standards, for the purposes of administering student conduct sessions.
		2. OSRR may utilize audio capabilities as stipulated above in section 9.1.

## Testing Center Video Cameras

* + 1. Any UCF testing center may utilize video cameras, within the guidelines of these standards, for the purposes of proctoring tests.
		2. University testing centers may utilize audio capabilities as stipulated above in section 9.1.

## Law Enforcement Video Cameras

* + 1. The UCF Police Department may utilize video cameras, within the guidelines of these standards, for the purposes of conducting subject interviews.
		2. The UCF Police Department may utilize audio capabilities as stipulated above in section 9.1 in interview rooms and the public lobby.
		3. The UCF Police Department interview rooms used to conduct subject interviews will be handled as law enforcement sensitive data by law enforcement officials.

## License Plate Recognition (LPR) Cameras

* + 1. License Plate Recognition hardware and software will be managed by the Department of Security in collaboration with the UCF Police Department and Parking Services.
		2. Access to LPR software is restricted to the Department of Security, UCF Police Department and Parking Services personnel.

# Appendix I: Acronyms, References & Definitions

## Acronyms

* + 1. **DS** – Department of Security
		2. **IP** – Internet Protocol
		3. **LPR** – License Plate Recognition
		4. **OSRR**- Office of Student Rights and Responsibilities
		5. **UCF** – University of Central Florida
		6. **VMS** – Video Management System

## Definitions

* + 1. **Administrators** – The Department of Security is the only authorized administrator of the Milestone Xprotect Corporate Video Management System.
		2. **Live Video** - A video feed showing a current, real-time live video image or images.
		3. **Milestone Xprotect Corporate –** The video management system utilized for the monitoring and recording of University video cameras.
		4. **Milestone Xprotect Management Client –** The software application used for the administrative controls and overall configuration of the Milestone Xprotect Corporate video management system.
		5. **Milestone Xprotect Smart Client –** The UCF-approved software application used for viewing live and recorded video.
		6. **Multipurpose Video Cameras -** A video camera serving additional purposes beyond general surveillance and security. This includes, but is not limited to: testing, conduct, law enforcement and license plate recognition (LPR) cameras.
		7. **Operator –** UCF personnel who are permitted access to the Milestone Xprotect Smart Client.
		8. **Recorded Image(s) -** Audio and/or video images captured by a video camera and stored for viewing at a later date.
		9. **University Video Camera(s)** - Any item, system, video camera, technology device, communications device, or process, used alone or in conjunction with a network, for the purpose of gathering, monitoring, recording or storing an image(s)of University facilities and/or people in University facilities. Images captured by University video cameras may be real-time or preserved for review at a later date. Such devices may include, but are not limited to the following: close circuit television, real-time surveillance systems, and computerized visual monitoring.

## References

* + 1. Florida Statute 1004.0962 <http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=1000-1099/1004/Sections/1004.0962.html>
		2. Florida Statute 119.011 <http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0100-0199/0119/Sections/0119.011.html>
		3. Florida Statute 119.017 <http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&URL=0100-0199/0119/Sections/0119.071.html>
		4. Florida Statute 281.301
		<http://www.flsenate.gov/Laws/Statutes/2012/281.301>