



UCF SECURITY CAMERA STANDARDS



**Department
of Security**

UNIVERSITY OF CENTRAL FLORIDA

Current as of:
December, 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. The DS's authorities and responsibilities are established in and executed in accordance with applicable federal and Florida laws 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 practices, plans, policies, and procedures. This position serves the University community by assisting campus administrators (senior leadership, staff, and faculty) with matters involving physical security. In addition, 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.

The purpose of the UCF Security Camera Standards is to provide the framework for the management and appropriate use of the video management system. In addition, it clarifies responsibilities and procedures for accessing, using, and modifying any part of the UCF security cameras or video management system.

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

TABLE OF CONTENTS

LETTER OF PROMULGATION.....	2
Chapter 1: General	5
Chapter 2: Responsibilities	7
Chapter 3: Violations and Sanctions.....	8
Chapter 4: Installation	9
Chapter 5: Maintenance.....	11
Chapter 6: Video Management System	12
Chapter 7: Video Management System Access.....	13
Chapter 8: Training.....	16
Chapter 9: Operation.....	17
Chapter 10: Multipurpose Video Cameras	20
Appendix I: Acronyms, References & Definitions.....	21

The University of Central Florida's Department of Security maintains these standards. 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

1.1. Purpose

- 1.1.1. To ensure the protection of individuals, property, and privacy rights in accordance with the University's core values and federal and Florida laws, this standard is adopted to formalize procedures for the handling, viewing, retention, dissemination, and destruction of recorded images. In addition, the purpose of this standard is to regulate the use of University security cameras and the video management system installed and operated in all UCF facilities and properties.

1.2. Principles

- 1.2.1 UCF is committed to using reasonable measures to mitigate potential threats and improve solvability factors related to crime on our campus. Critical components that assist in this endeavor are security cameras and other image capture tools.
- 1.2.2 UCF's Department of Security reserves the right to place security cameras where necessary and appropriate. The Department of Security respects the right to privacy of the University community (Section 9.6).
- 1.2.3 Security cameras provide a visual deterrent to crime and assist with overall security measures. Security cameras are not a guarantee of safety; however, they serve as deterrents and can assist the UCF Police Department and Department of Security in identifying potential danger. The primary use of security cameras is to record images for identification of individuals and activity in the event of violations of law or University regulations or policies.
- 1.2.4 University security cameras are not monitored continuously under normal operating conditions. However, they 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.
- 1.2.5 UCF also utilizes video cameras for other purposes such as to support education, research, and health care, which are exempt from these standards as listed in Section 1.3.3. Exempt video cameras are still required to adhere to all applicable Florida and federal laws, including retention guidelines.
- 1.2.6 All recording or monitoring of activities by University security cameras shall be conducted in a professional, ethical, and legal manner consistent with University regulations and policies, Florida 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.
- 1.2.7 Departments installing a video camera system (hardware, software, or related equipment) for purposes outlined in Section 1.3.3 and capable of viewing public areas or entrances/exits, whether it's connected to the network or an isolated system, must complete the UCF Educational/Research Video Camera Information Form located at <https://police.ucf.edu/securitycameras>. This includes video cameras purchased with department

funds, grants, or any other UCF funding source. The UCF Educational/Research Video Camera Information Form collects contact information for the individual(s) responsible for managing the exempt system, which will assist UCF Public Safety in obtaining footage of evidentiary value for investigating crimes. This form will not collect information regarding how to access cameras; UCF Public Safety personnel will work with the identified point(s) of contact to review footage.

1.3. Scope

- 1.3.1. All University community members (students, faculty, staff, and guests), those doing business at the University, and those on a university-controlled property must comply with these standards.
- 1.3.2. Specific video cameras may be exempt from these standards. However, individual(s) operating these video cameras are still responsible for adhering to all applicable Florida and federal laws, including retention requirements and necessary consent. Questions about federal and state requirements should be directed to the UCF Office of the General Counsel.
- 1.3.3. Exemptions to these standards include, but are not limited to:
 - 1.3.3.1. Video cameras used for journalistic purposes;
 - 1.3.3.2. Video cameras used for broadcasting public events or performances;
 - 1.3.3.3. Video cameras used to record musical or theatrical performances;
 - 1.3.3.4. Video cameras located in clinical or treatment areas, including those that are covered by the approved HIPAA Compliant Camera Centralization Procedures;
 - 1.3.3.5. Video cameras installed or used in an office, classroom, or laboratory with controlled access, and surveil for non-security purposes (refer to Section 1.2.7);
 - 1.3.3.6. Video cameras used for web or video conferencing, marketing, and recruitment;
 - 1.3.3.7. Video cameras connected directly to mobile devices such as smartphones, tablets, and laptops;
 - 1.3.3.8. UCF Police body cameras, which are used in accordance with Florida Statute 943.1718;
or
 - 1.3.3.9. Video cameras located in UCF Police Department patrol vehicles.

CHAPTER 2: RESPONSIBILITIES

2.1. Department of Security Responsibilities

2.1.1. The Department of Security is responsible for:

- 2.1.1.1. the realization, assimilation, and enforcement of these standards;
- 2.1.1.2. reviewing and approving or denying any requested exception to these standards that currently is not listed in Section 1.3.3;
- 2.1.1.3. proposing appropriate changes to these standards to the Associate Vice President and Chief of Police, as needed;
- 2.1.1.4. selecting and administering the approved video manage system (VMS);
- 2.1.1.5. advising departments on appropriate applications of camera technologies and for assisting departments preparing for the purchase and installation of security cameras;
- 2.1.1.6. monitoring developments in federal and Florida laws, current trends in technology, and continuing to implement best practices;
- 2.1.1.7. reviewing and approving proposals for security camera installations, as well as reviewing specific security camera types and locations to ensure the best view and image quality is captured;
- 2.1.1.8. maintaining and testing security camera hardware and software;
- 2.1.1.9. maintaining log files indicating users who access the camera client; and
- 2.1.1.10. reviewing any complaints regarding the operation of security cameras and determining whether these standards are being followed.

2.2. Operator Responsibilities

2.2.1. Operator is responsible for:

- 2.2.1.1. performing duties in accordance with these standards,
- 2.2.1.2. accessing live video or recorded images only to the extent permitted by these standards, and
- 2.2.1.3. notifying the Department of Security if a security camera is not functioning properly.

CHAPTER 3: VIOLATIONS AND SANCTIONS

3.1. Sanctions

- 3.1.1. Failure to comply with these standards could result in one or more of the following, but not limited to:
 - 3.1.1.1. Loss of security camera access privileges;
 - 3.1.1.2. Institutional sanctions up to and including termination of employment; and
 - 3.1.1.3. Legal action.
- 3.1.2. Any person who tampers with, damages, or destroys security camera equipment will be subject to applicable criminal proceedings and disciplinary action.
- 3.1.3. Unauthorized, unethical, or illegal use or installation of a security camera in violation of these standards may subject an employee, student, or guest to applicable disciplinary action and criminal proceedings.

3.2. Reporting

- 3.2.1. Concerns about possible violations of these standards related to inappropriate use of security cameras or the video management system should be directed to the Department of Security.

CHAPTER 4: INSTALLATION

4.1. Installation, Relocation, and Removal

4.1.1. Requests for installation, relocation, and removal of security cameras in/on University property must be coordinated with and approved by the Department of Security.

4.1.1.1. Installations of security cameras in/on new building construction or building renovations must be coordinated with the Department of Security and Facilities Planning and Construction.

4.1.1.1.1. Renovations exceeding 50% of a building's space require the entire renovation meets current Department of Security recommendations for security camera installations.

4.1.1.1.1.1. Space percentage is determined by Facilities Planning and Construction

4.2. Processes

4.2.1. Requests for installations of new security 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>.

4.2.2. Requests for relocating, repositioning, upgrading, changing, and removing security cameras must be submitted to the Department of Security using the *UCF Camera Maintenance Request* form located at <http://police.ucf.edu/securitycameras>.

4.2.3. 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. 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.

4.2.4. The department or college requesting security cameras will be responsible for the initial cost of the security camera, storage hardware, and related installation costs of hardware and supporting network, as well as initial software licensing fees. If security cameras are required in a new construction or major renovation project, associated costs shall be funded by the project. The Department of Security will help identify additional costs associated with the security camera project, upgrade, or installation.

4.3. Departments requesting grant funding to add or alter any new or existing security cameras or systems must obtain prior approval from the Department of Security.

4.3.1. Any grant or technology fee proposal for additional security camera equipment or modification to existing camera equipment must comply with all associated standards, including UCF Security Camera Standards.

- 4.4. All new installations of security cameras scheduled after the effective date of these standards must comply with the terms and conditions of these standards.
- 4.5. The Department of Security will oversee the physical installation of all pre-approved security camera hardware.
- 4.6. Unless required by the Department of Security or Office of the General Counsel, signage indicating the existence of a nearby security camera is not required. If a department or college wishes to install signage at their own expense, only specific, approved language is permitted, which should not be altered without approval from the Department of Security.
 - 4.6.1. Signage must read: **CAMERA[S] LOCATED IN [BUILDING/SUITE/ROOM]**
 - 4.6.1.1. Example 1: **CAMERA LOCATED IN ROOM**
 - 4.6.1.2. Example 2: **CAMERAS LOCATED IN SUITE**
 - 4.6.2. Existing signage with alternate wording must immediately be replaced by the department or college assigned to the building, suite, or room.
- 4.7. It is prohibited to install “dummy” or false (fake) security cameras that do not operate. These cameras can increase the university's liability and create a false sense of security.
- 4.8. The department or college in possession of security cameras that are no longer functional must remove all devices and related hardware at their own expense and per UCF IT Telecommunications and Facilities Planning and Construction standards.
- 4.9. Security camera equipment, devices, or systems installed without appropriate authorization after the effective date of these standards will be immediately disabled upon notice if not reauthorized under these standards. Violating cameras and associated equipment will be removed at the expense of the department found to be responsible.
- 4.10. The UCF Police Department will publish in their Annual Crime Report information regarding the number of investigations where security cameras are used to assist.

CHAPTER 5: MAINTENANCE

- 5.1 All security 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 security camera must be done by a UCF Department of Security-approved vendor or contractor. At no time shall any UCF personnel perform physical maintenance on security cameras unless authorized to do so by the Department of Security.
- 5.3 If a security camera can longer be maintained, the Department of Security may require its removal or replacement.
- 5.4 If a department will be responsible for funding security camera maintenance (including removal or replacement), associated costs will be communicated to and approved by the funding department prior to proceeding.

CHAPTER 6: VIDEO MANAGEMENT SYSTEM

- 6.1. The UCF Department of Security centrally manages security camera systems.
- 6.2. The Department of Security selects and administers the approved video management system used to record and access footage from security cameras. All new University security camera hardware must operate on this approved video management system.
- 6.3. Security camera systems installed prior to the original effective date of these standards shall be immediately configured to provide management and viewing access to the DS and transition into the University's video management system. Departments operating these systems are required to adhere to all Florida and federal laws, including retention guidelines, until they can be removed or replaced with cameras on the approved video management system.

CHAPTER 7: VIDEO MANAGEMENT SYSTEM ACCESS

7.1. University Security Camera Access

- 7.1.1. Accessing a physical security camera by any means other than using the approved video management system is only permitted to those authorized by the Department of Security.
- 7.1.2. The alteration of any hardware, software, or network feature of a University security camera is only permitted to those authorized by the Department of Security. Departments interested in altering security camera features shall consult with the Department of Security to determine appropriateness.
- 7.1.3. The alteration of the physical network infrastructure connected to any University security camera is only permitted by UCF IT Telecommunications personnel in partnership with the Department of Security.

7.2. Management Client

- 7.2.1. The management client is the software used to manage the administrative controls and overall configuration for the video management system.
- 7.2.2. Access to the management client is only permitted to Department of Security personnel.
- 7.2.3. Approved personnel within UCF IT may have access to the physical and virtual servers hosting the video management system. However, accessing any video management system software by UCF IT or any person outside of the Department of Security without the Director of Security Management's approval is strictly prohibited.

7.3. Camera Client

- 7.3.1. The camera client is the software used by Operators to view live video and recorded images from security cameras.
- 7.3.2. Anyone requesting access to the camera client must obtain authorization from the Department of Security. Requests must be made using the *Camera Client Access Request* form located at <http://police.ucf.edu/securitycameras>.
- 7.3.3. Only personnel approved and trained to use the video management system are permitted to operate the camera client. Failure to comply may result in punitive actions by UCF.
- 7.3.4. Operators of the camera client are prohibited from:
 - 7.3.4.1. Sharing their password 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.

- 7.3.4.2. Viewing the interior of residential rooms, offices, or locations with a reasonable expectation of privacy, through windows, doors, or other means. Security cameras shall not be directed at the windows of any privately-owned residence, residential rooms, offices, or locations with a reasonable expectation of privacy.
- 7.3.4.3. Duplicating images or permitting access to others except as specifically permitted by these standards.
- 7.3.4.4. Viewing, recording, accessing, or otherwise using the video management system in any manner that is inconsistent with these standards or outside the scope of the usage approved by the DS.
- 7.3.4.5. Discussing with others any details regarding what they view in any live or recorded footage unless there is a business need related to campus safety and security.

7.3.5. The information below identifies the different camera client access levels for Administrators and Operators:

Security Level	Export (download footage)	Playback/Recorded Images	Live Camera Feeds	Management Client/System Administration	ALL UCF Security 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

- 7.3.6. Security Level 1 or administrative access is permitted only to the Department of Security (DS) personnel. Access is assigned by the Director of Security Management.
- 7.3.7. Requests for public records release related to recorded images and video must be immediately directed to the Department of Security. Operators must not release recorded images or video in response to a public records request (see Section 9.4).

- 7.3.8. 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 Management.
- 7.3.8.1. 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/securitycameras>. All suspected or confirmed criminal activity must be reported immediately to the UCF Police Department at (407) 823-5555. The Detective assigned to the case will have the ability to obtain security camera footage stored on the video management system.
- 7.3.9. 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. Additional authorized users are approved by the Associate Vice President and Chief of Police, and the Director of Security Management.
- 7.3.10. UCF employees may request access to view live video located within their respective departments by submitting the access request form at <http://police.ucf.edu/security>.
- 7.3.10.1. Access requests will be reviewed and accepted or rejected by the Department of Security based on the business justification provided.
- 7.3.11. For access permissions to License Plate Recognition devices, see section 10.4.

CHAPTER 8: TRAINING

- 8.1. Those who have been approved to use the camera client will be trained in the requirements of these standards and the technical and ethical parameters of appropriate security camera use. Training will be led by Department of Security personnel.
- 8.2. Training for the Operators will be scheduled and conducted once the access request form is submitted to and approved by the Department of Security. The form is located at <http://police.ucf.edu/securitycameras>.
- 8.3. Each camera client Operator must complete the Camera Client End-User Training provided by the Department of Security.
- 8.4. Access will not be granted to the Operator prior to completing the required training courses stipulated in section 8.3.
- 8.5. Operators of the video management system will receive a copy of these standards and provide an acknowledgement that 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 Security Camera Standards. All revisions will be posted to <http://police.ucf.edu/securitycameras>.

CHAPTER 9: OPERATION

9.1. Audio

- 9.1.1. Audio recordings shall be prohibited unless specifically requested by a department and authorized by the Department of Security.
- 9.1.2. Multipurpose video cameras may record audio once authorized by the Department of Security.
- 9.1.3. Signage must be posted in UCF spaces where there is audio recording of faculty, staff, students, or guests.
 - 9.1.3.1. 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

9.2. Covert Video

- 9.2.1. The use of covert video may only be used in special and unique circumstances. This use must be approved by the Associate Vice President and Chief of Police, and Director of Security Management.

9.3. Protection & Retention of Recorded Images & Audio

- 9.3.1. Alteration
 - 9.3.1.1. No attempt shall be made to alter any part of recorded images.
 - 9.3.1.2. The use of personal recording devices and third-party software (including but not limited to: cell phones, camcorders, Skype, Teams, and tablets) to record live video or recorded images from our video management system is strictly prohibited.
- 9.3.2. Recorded Images & Audio Storage
 - 9.3.2.1. Recorded images and audio from security cameras shall not be stored by individual departments unless authorized by the Department of Security.
 - 9.3.2.2. Recorded images and audio from security cameras 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.
 - 9.3.2.3. Recorded images from security cameras will be stored for a minimum period of 30 days and thereafter may be erased.

- 9.3.2.4. A request must be submitted to the Department of Security for security cameras to retain recordings for longer than 30 days.

9.4. Release of Recorded Images

- 9.4.1. Recorded images from security cameras 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 Management.
- 9.4.2. The unauthorized release of recorded images from security cameras is strictly prohibited and could result in disciplinary action, as referenced in Section 3.1.
- 9.4.3. UCF personnel and departmental requests for recorded images from security cameras must be submitted to the Department of Security. No department personnel, including the dean, director, or designated executive authority, can authorize the release of recorded images.
- 9.4.4. Recorded images under active, or may be under future, law enforcement investigation, audit or compliance investigations, or other UCF investigations will not be released to any party without approval from the investigating authority.

9.5. Audit

- 9.5.1. 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 security cameras and the video management system. The log shall include the date and identification of the person(s) to whom access was granted.

9.6. Expectation of Privacy

- 9.6.1. Operators of the camera 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 (see Section 7.3.4.2).
- 9.6.2. Where security 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.

- 9.6.3. 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 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

10.1. Student Conduct Video Cameras

- 10.1.1. The Office of Students Rights & Responsibilities (OSRR) may utilize video cameras, within the guidelines of these standards, for student conduct sessions.
- 10.1.2. OSRR may utilize audio capabilities as stipulated above in section 9.1.
- 10.1.3. UCF Public Safety does not actively monitor these cameras.

10.2. Testing Center Video Cameras

- 10.2.1. Any UCF testing center may utilize video cameras, within the guidelines of these standards, to assist with proctoring tests.
- 10.2.2. University testing centers may utilize audio capabilities as stipulated above in section 9.1.
- 10.2.3. UCF Public Safety does not actively monitor these cameras.

10.3. Law Enforcement Video Cameras

- 10.3.1. The UCF Police Department may utilize video cameras, within the guidelines of these standards and in accordance with applicable Florida and federal laws, accreditation standards, and relevant case law to conduct subject interviews.
- 10.3.2. The UCF Police Department may monitor or record audio as stipulated above in section 9.1, applicable Florida and federal laws, accreditation standards, and relevant case law.
- 10.3.3. The UCF Police Department recordings from interview rooms used to conduct subject interviews will be handled as law enforcement sensitive data by law enforcement officials.

10.4. License Plate Recognition (LPR) Cameras

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

APPENDIX I: ACRONYMS, REFERENCES & DEFINITIONS

1.1. Acronyms

- 1.1.1 **DS** – Department of Security
- 1.1.2 **LPR** – License Plate Recognition
- 1.1.3 **OSRR**- Office of Student Rights and Responsibilities
- 1.1.4 **UCF** – University of Central Florida
- 1.1.5 **VMS** – Video Management System

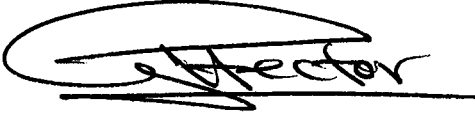
1.2. Definitions

- 1.2.1 **Administrators** – The Department of Security is the only authorized administrator of the video management system.
- 1.2.2 **Camera Client** – The UCF-approved software application used for viewing live and recorded video.
- 1.2.3 **Live Video** - A video feed showing a current, real-time live video image or images.
- 1.2.4 **Management Client** – The software application used for the administrative controls and overall configuration of the approved video management system.
- 1.2.5 **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.
- 1.2.6 **Operator** – UCF personnel who are permitted access to the camera client.
- 1.2.7 **Recorded Image(s)** - Audio and/or video images captured by a video camera and stored for viewing at a later date.
- 1.2.8 **University Security Camera(s)** or **Security Camera(s)** – A University video camera primarily used to enhance campus safety and security.
- 1.2.9 **University Video Camera(s)** or **Video Camera(s)** - Any item, system, 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 occupying these 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.

1.3. References

- 1.3.1 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
- 1.3.2 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
- 1.3.3 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
- 1.3.4 Florida Statute 281.301
<http://www.flsenate.gov/Laws/Statutes/2012/281.301>
- 1.3.5 Florida Statute 943.1718
http://www.leg.state.fl.us/statutes/index.cfm?mode=View%20Statutes&SubMenu=1&App_mode=Display_Statute&Search_String=943.1718&URL=0900-0999/0943/Sections/0943.1718.html
- 1.3.6 Case: Riley v. State, 2013 WL 275272 (Fla. 5th DCA 2013)
<http://www.fdle.state.fl.us/getattachment/1cf1497b-6b30-433a-9278-3ad8a3a87600/01>
- 1.3.7 UCF Office of the General Counsel
<http://generalcounsel.ucf.edu>

UNIVERSITY APPROVALS

Title	Print Name	Sign Name	Date
Senior Vice President, Administration and Finance	Gerald Hector		3/1/2022
Associate Vice President of Safety and Security / Chief of Police	Carl Metzger	Carl Metzger <small>Digitally signed by Carl Metzger Date: 2022.01.03 12:53:17 -05'00'</small>	01/03/2022
Director, Security Management	Steven Freund	Steven M. Freund <small>Digitally signed by Steven M. Freund Date: 2021.12.10 12:02:15 -05'00'</small>	12/10/2021
Provost (or designee)	Michael Johnson	Michael Johnson <small>Digitally signed by Michael Johnson Date: 2021.12.10 14:01:02 -05'00'</small>	12/10/2021
General Counsel (or designee)	Youndy C Cook	Youndy C. Cook <small>Digitally signed by Youndy C. Cook Date: 2022.01.03 12:03:03 -05'00'</small>	01/03/2022