UNIVERSITY OF CENTRAL FLORIDA

Office of the President

SUBJECT:	**Effective Date:**	**Policy Number:**
University Access Control	5/6/2022	3-105.1
	Supersedes: 3-105	**Page** 1 **Of** 12
	Responsible Authority: Assistant Vice President for Facilities Operations; Associate Vice President for Public Safety and Chief of Police	

APPLICABILITY/ACCOUNTABILITY

This policy applies to anyone issued or authorized to access secured university spaces on all university campuses via physical keys or electronic access card, included but not limited to university employees, students, and contractors working on campus.

This policy excludes student room keys and electronic card access issued by Housing and Residence Life.

POLICY STATEMENT

The University of Central Florida strives to provide appropriate security to university spaces through access management and control. This policy prescribes the offices responsible for access control and provides procedures for providing access to employees, students, and contractors working on campus. Access Control is managed by the Division of Administration and Finance. Electronic Access Control follows a single, unified approach, using only the university approved Electronic Access Control System(s), administered by the Department of Security. Physical key control is administered by Facilities & Business Operations (F&BO).

The Department of Security is responsible for the installation, maintenance, modification,

and administration of the university approved Electronic Access Control System in university facilities. Disparate access control systems may continue to be utilized for existing doors, but cannot be added, expanded, or replaced without written authorization from the Department of Security.

Access

Electronic access should be used as a primary means of entry, where available. Spaces on electronic card access control must only be able to be opened by GGM or Building Master. UCF Cards are the only cards authorized for electronic card access to buildings and rooms on campus. Any exceptions must be approved in writing by the Department of Security. Employees may be issued physical keys to access their workspaces. The university strongly advises against the issuance of physical keys to students, however, should a department require this, the request should be submitted through the online key request system. Keys will not be issued to volunteers. F&BO will process all physical key requests, transfers, replacements, and returns. An electronic access card holder or physical key holder may not give away, loan, or swap access cards or physical keys, and must immediately notify their supervisor if an access card or physical key is lost or stolen. Lost or stolen Building Sub-Master, Building Master or GGM keys will not be replaced until a report has been filed with the UCF Police Department. Upon separation from the university, electronic access will be terminated, and employees must return all university physical keys to their University Access Control Representative (UACR).

The Department of Security will ensure all new electronic access control hardware utilizes the university's approved electronic access control system and is purchased from the university's contracted vendor. Other access control systems may continue to be used for existing doors but cannot be expanded or replaced without authorization from the Department of Security. New electronic access control systems that do not use the university's approved system are prohibited, unless approved by the Department of Security.

All doors with electronic access control must also be on the university physical key system and be accessible only by the Building Master or GGM, unless approved by the director of Security Management, AVP of FO, and the director of Environmental Health & Safety (EH&S).

Doors which protect critical infrastructure, as identified by the Department of Security, F&BO, and UCF IT, will require electronic access with two-factor authentication (such as requiring card and PIN) for entry, unless the installed hardware does not support it. All electronic access control hardware that does not protect critical infrastructure, as determined by the Department of Security, may be configured to require "card only" authentication or two-factor authentication.

Modifications to existing buildings or rooms that might result in adding or moving entrances must be reviewed by the Department of Security to determine whether electronic access control should be added, modified, or removed.

Only the FO Lock Shop (Lock Shop) may duplicate university physical keys or install/maintain mechanical locking hardware to university spaces. Any other method of key duplication, lock installation or rekeying is prohibited.

Individual Responsibilities

Whenever possible, individuals should access buildings and rooms using electronic access. Physical key should only be used in emergency situations. No self-closing doors should ever be propped open to bypass the access control. Upon accessing a controlled space, the individual must recognize the current state of the lock and ensure the lock is in the same state upon exiting. If a sensitive controlled space is found to be in an unlocked state, the individual must secure the space and report the incident to the building liaison.

The UACR must regularly monitor and periodically inspect the electronic access control hardware in their building(s) and report any issues to the Department of Security. Individual users must immediately notify the Department of Security if a door and/or system is not functioning as intended.

Individuals with electronic access shall not share their physical keys, access cards, and/or PINs with any other individual.

Individuals who lose their UCF Card must immediately report it to their supervisor and the UACR.

Non-University Locks

No locks may be installed on a university building or property without an approved Non-University Lock Approval Form from AVP of FO and being added to the University Key System. Locks installed without an approved form will be removed at the department's expense.

Prohibited Actions

Actions violating this policy include, but are not limited to:

- Loaning a university physical key or electronic access card to another individual
- Obtaining and issuing a physical key or electronic access card without authorization
- Duplicating or attempting to duplicate physical keys or electronic access cards
- Damaging, tampering, vandalizing, altering, or modifying university access devices, hardware, locks, or other access mechanisms
- Installing or causing to be installed an unauthorized locking mechanism on university spaces (e.g., offices, labs, etc.)
- Propping doors open to avoid the use of access devices
- Admitting unauthorized person(s) into a building
- Failing to return a physical key when requested by FO, the UACR, or upon leaving

employment with the university
- Failing to report missing physical keys or electronic access cards
- Failing to return a Building Master or GGM key within the 12-hour curfew

Violations of this policy may result in the loss of electronic card access privileges and/or physical key issuance, charges for lost physical keys or for rekeying areas and buildings. Individuals determined to have violated this policy may be subject to disciplinary action, up to and including termination. Contractors who violate this policy may lose access to a space, the campus, or the university may sever the business relationship.

DEFINITIONS

Building Master Key. A physical key that accesses any lockset, with the exception of mechanical/electrical, telecom, and roof locks, in a specific building.

Building Sub-Master Key. A physical key that accesses a lockset in an area/suite within a specific building. Includes the Suite Master Key.

Critical Infrastructure. Assets, systems, and networks, whether physical or virtual, that are essential to the university, and are so vital that their incapacitation could cause significant disruption or harm to people, property, and university operations. Examples of critical infrastructure include, but are not limited to: the water and wastewater supply, electrical power transmission and distribution, chilled water, natural gas distribution, telecommunications, and information technology, as well as rooms or areas containing mechanical, electrical, telecom, utility, and elevator control equipment.

Electronic Access Card. UCF-issued access card that allows entry to one or more university buildings and/or rooms.

Electronic Access Control. Selective restriction of access to buildings or rooms using authentication methods including, but not limited to, identification cards, personal identification numbers, and biometrics.

Electronic Access Control Hardware. The physical equipment required to facilitate electronic access.

Electronic Access Control System. The software used for electronic access to buildings and rooms.

Electrical or Mechanical Room Key. A physical key that accesses electrical and mechanical rooms.

Great Grand Master (GGM) Key. The highest level of physical key in the university physical keying system, allowing unlimited access to all spaces on the university physical key system.

Janitor Key. A physical key that accesses janitorial rooms.

Leased Space Key Representative. A non-UCF employee occupying a UCF owned space via a lease agreement who manages the key request process and maintains key records for the non-UCF entity under a UCF sponsored account.

Loaning. Temporarily allowing a key or Electronic Access Card that is assigned to a specific employee, or that can be accessed by that employee in a physical key security box, to be used by another individual.

Physical Key. A piece of shaped metal that is inserted into a lock to open or close the locking system.

Room (Space) Key. A physical key that accesses a specific room within a university building.

Sponsored Account. The method by which a full-time UCF employee can provide a non-UCF individual/company a UCF Network ID (NID) to obtain access to applicable UCF systems for a defined period of time.

Suite. A set of connected rooms, serviced by a common locked entrance.

UCF Card. The official identification card used to identify an employee or student's affiliation with the university, used for electronic access.

University Access Control. The physical or electronic lock system owned by UCF.

University Access Control Representative (UACR). An A&P or USPS employee who manages physical key requests and electronic card access for a specific department, unit, or building, and maintains key records for their department or area. UACRs are appointed by a dean, director, or chair, through a written request to Facilities Operations (FO). For electronic card access provisioning privileges, the UACR must be approved by the Department of Security and successfully complete the required training. A list of current UACRs is posted at fo.ucf.edu.

PROCEDURES

1. Approvals

Different access types provide varying levels of entry to university spaces and, therefore, require different levels of approval. The approval paths for each access type are as follows:

Access Type	UACR	Dean, Director, Chair	Lock Shop or Facilities Asset Management*	Director, FO	IT Telecom	AVP of FO, or Chief of Police
Great Grand Master (GGM)	X	X	X	X		X
Building Master	X	X	X	X		
Building Sub-Master (Suite)	X	X	X			
Room/Space	X	X	X			
Electrical, Mechanical Room	X	X	X	X		
Roof	X	X	X	X		
Janitor	X	X	X	X		
Telecom	X	X	X	X	X	

*Approval required for physical key issuance only.

NOTE: Individuals should only be granted access to buildings and rooms required for them to perform their daily job functions.

2. Access Requests

a. Electronic Access Requests

Departments will develop an internal procedure to document and manage adding, modifying, or removing electronic access within their area(s), including delineating the responsibilities of requestors, the UACR, and departmental approvers.

The requestor will submit a request to the UACR, who will obtain all necessary approvals. The UACR will then add, remove, or modify the individual's electronic access. UACRs may not grant access to rooms managed by other units.

All UACRs requiring access to the electronic access control software are required to attend formal training, facilitated by the Department of Security, before receiving access.

The appropriate F&BO department must approve electronic access requests for master access or access to mechanical rooms, utility corridors, utility generation facilities, electrical rooms, elevator control rooms, rooms that are not accessible using a university key GGM, etc. UCF IT must approve requests for telecommunications equipment rooms. Electronic access to all other spaces is managed and approved at the department level.

b. Physical Key Requests

Persons requesting a new or replacement physical key will submit a request to their UACR, who will submit it through the online key request system, along with the appropriate documentation.

In order to be issued access to a GGM, Electrical, or Mechanical key, the person for whom the key is being requested must complete EHS training course 690, Electrical and Mechanical Room Safety at UCF, and submit the certificate of completion to his or her UACR.

Contractors requiring keys must submit a Key Request Letter to the university contact managing the project, who will then forward to the appropriate UACR for approval, in accordance with the chart below. The UACR may grant access to contractors on either an annual or project-specific basis. Access may not be granted for longer than one calendar year. Approved Key Request Letters will be kept on file in the Facilities Resource Center (FRC).

Contractor	Annual Physical Key Request	Project-specific Physical Key Request	Physical Key Request Type
Elevator, Fire Alarm	X		GGM
Utilities, Architects, MEP Engineers, General Contractors, Construction Managers	X	X	GGM, Building Master, Mechanical, Electrical, Roof
Continuing Services Contractors (CSC)		X	Building Master, Roof
Non-CSC contractors		X	Building Master, Roof

3. Electronic Access Issuance

UACRs must perform an annual review of all individuals with electronic access to their buildings and rooms and update as necessary. The results of the review should be maintained by the unit and provided to the Department of Security upon request.

Authorized F&BO employees will be given electronic access to all the areas in which they perform their job functions. Authorized IT employees will be given access to any telecommunications rooms with electronic access. Once an individual is approved for GGM access through the online key request system, corresponding GGM electronic card access will be provisioned.

Doors configured to follow a time schedule will also be configured to follow the university's holiday schedule, to remain secured when the university is closed. Doors can also be configured to remain secured during an emergency closure. The Department of Security will grant electronic access to first responders and other individuals, as required.

UACRs must revoke an individual's access to buildings immediately upon termination. When an employee transfers to a different department, the need for continued access must be evaluated and modified as appropriate. If a UCF Card is lost, all access levels must be immediately removed until a replacement card is issued.

The Department of Security is the official custodian of all access control records. Any external or public record requests for access control data should be immediately forwarded to the Department of Security.

4. Electronic Access Control Hardware Installation and Maintenance

Requests to add electronic access control hardware to existing buildings and rooms shall be initiated by contacting the Department of Security. Upon approval, the requesting department will submit a Minor Project request through Facilities Planning & Construction (FP&C). Existing classrooms, teaching and research laboratories, conference rooms, or common rooms with high-valued computer equipment or technology, as determined by the Department of Security, will require electronic access control hardware should the room undergo a Minor Project through FP&C. The unit or department installing the electronic access control hardware shall be financially responsible for installation.

All new construction will be evaluated by the Department of Security during the design phase, to determine where electronic access control will be installed and what hardware is required. The project will fund electronic access control for exterior doors, critical infrastructure, suite entry doors, classrooms, laboratories, conference rooms, rooms with high-value items, and secure storage areas. All access control installations will adhere to the most recently published UCF construction standards.

5. Physical Key Issuance

All physical keys are engraved with a code to identify the key holder and type of key. Only one key will be issued to each person for each space. Multiple keys must be requested individually, and a separate Key Request Form must be filled out for each person requesting keys. For suites with more than 24 doors, a maximum of two Building Sub-Master (Suite) keys will be issued to individuals; any additional requested Suite keys must be housed in a key security box. Additional Suite keys are only allowed for suites with 24 doors or less.

The key must be picked up in person at the FRC, located in F&BO (Building 16A), within 30 days of notification that the key is ready. If the person to whom the key is assigned is unable to retrieve the key, a representative from their unit may pick it up by providing his/her name and employee ID number. Keys not picked up within 30 days will be returned to the Lock Shop, and a new Key Request Form must be submitted. Keys are billed when the Lock Shop processes the Key Request Form; therefore, additional charges will be incurred for new key requests.

Room and Suite Master keys for non-UCF entities who are leasing UCF space will be issued to an appointed Leased Space Key Representative, using a Sponsored Account. The Representative will be responsible for managing key assignments and complying with all inventory requests.

GGM and Building Master keys are issued to key security boxes via a work order, not individuals. Approved individuals may check out a GGM or Building Master key from a designated key security box during their work shift. Anyone authorized to use a GGM, or Building Master key must exercise extreme vigilance in protecting it at all times. Employees and contractors who have been approved to use a GGM or Building Master key will be assigned a key security box location from which to access the appropriate key. GGM keys may not be taken off campus. Any exception for issuance of a Building Master key to an individual must be approved in writing by the AVP of FO.

When contractors report to the FRC to obtain keys, they will be required to show a picture ID, and FRC will retrieve the appropriate key(s) for the contractor. For satellite campuses, an electronic access card will be provided to each approved individual listed on the Key Request Letter for the duration of the project that will allow the individual access to the key security box at the satellite campus. If a project's timeline is extended, the contractor may request extended access by updating the original Key Request Letter and submitting through the UCF representative. However, if the initial access period has already expired, or if it's going to extend past a year, the contractor must submit a new Key Request Letter.

All Building Master, Electrical, Mechanical, Roof, and Great Grand Master keys must be returned to the FRC within 12 hours of checkout.

Employees within the UCF Police Department who are authorized to remove a GGM key from campus or authorized to override the 12-hour curfew must have an approved GGM Exception Form.

6. Key Transfers and Returns

To transfer a physical room key to another individual, the original key must be returned to the UACR. The UACR will fill out the Key Transfer Request Form and submit it, along with the physical key(s), to the FRC. Only room keys may be transferred; all other keys require additional approval. Key transfers should only occur when there is an immediate recipient; otherwise, the UACR must complete a Key Return Form.

When a key is no longer required, it must be returned to the keyholder's UACR, who will complete a Key Return Form and submit it, along with the key, to FRC. This will facilitate the key being removed from the individual's university records. Failure to return a key upon separation from the university may result in departmental charges, if a rekey of the space is deemed necessary by the AVP of FO or the Chief of Police.

7. Rekeying

Rekeying of locks will be requested via a work order. The cost to rekey is at the requestor or department's expense.

When an area requires additional security or confidentiality, a Request for Exemption from the University Key System to rekey a door off of the campus GGM must be submitted to and approved by the AVP of FO and the Chief of Police. The area will be put on the university approved electronic access control system, at the department's expense, and access must be provided to UCF Police Department for emergency purposes.

8. Physical Key Control

With the exception of the UCF Police Department, physical key control is facilitated through the use of a physical key control box approved by the AVP of FO. Physical key control boxes that are not approved by the AVP of FO are prohibited. If unapproved key control boxes are found, they will be removed at the department's expense.

Departments requiring a key control box must purchase the box through F&BO, through a chargeable work order. The department will also be responsible for permitting fees, material and installation charges, ongoing administrative fees, licenses, and maintenance.

Key control boxes managed by departments other than F&BO that contain GGM, Building Master, Electrical, Mechanical or Roof keys will have security measures in place to prevent the box administrator to access these keys, unless additional approvals are obtained.

9. Key and Lock Charges

Departments are responsible for the cost of new keys, replacement keys, failure to return keys, and rekeying of areas or buildings. The cost to rekey will be based on the actual materials and labor required to complete the request, as set forth at https://fo.ucf.edu/labor-rates/. Worn keys will be replaced at no charge and the original key must be returned to the FRC. Keys not returned to the FRC will be billed as lost.

10. Key Records and Audits

- The Lock Shop will maintain individual key records.
- Departmental key reports are available to the UACR in the University Key System.
- All university keys must be returned to the UACR when an employee separates from the university, transfers departments, changes room assignments, or upon request from the Lock Shop.
- FRC will retain copies of all active contractor Key Request Letters and will notify the appropriate UCF representative when a contractor's Key Request Letter is one week from expiration.
- FO will periodically perform physical inventories of keys, including departmental key control boxes. Departments will be charged for missing keys.

RELATED INFORMATION

Department of Security Website: http://police.ucf.edu/security
Key Forms: https://fo.ucf.edu/key-request-information/
Minor Project Request Form: https://fp.ucf.edu/resources/request-forms/

INITIATING AUTHORITY

Senior Vice President for Administration and Finance;
Vice President of Facilities and Business Operations

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: 3-105.1

Initiating Authorities: _____ Date: 5/3/22

Jonathan Varnell
Digitally signed by Jonathan Varnell
Date: 2022.05.04 14:15:27 -04'00'

_____ Date: 5/4/2022

University Policies and Procedures Committee Chair: _____ Date: 4/29/22

Alexander Cartwright
Digitally signed by Alexander Cartwright
Date: 2022.05.06 07:30:18 -04'00'

President or Designee: _____ Date: 5/6/2022

History: 3-105, 12/7/2017