University Compliance, Ethics, and Risk Office

UNIVERSITY OF CENTRAL FLORIDA

University of Central Florida
Draft Policy Submission Cover Memo Form

Policy No. and Title: UCF 3-105.2 University Access Control

Initiating Authority: Vice President for Operations

Initiating Authority Approval Date: 10/24/25

Date of Submission for Review: 5/21/2026

Submitted by: Assoc. VP Utilities and Engineering Services and Chief Engineer and Assoc. VP of Public Safety

Department: Facilities and Business Operations and Public Safety

☐ New Policy ☑ Existing Policy (5-year Review) ☐ Existing Policy (Out of Cycle Review)

Summary of Revisions: (For a new policy, please provide a summary of the policy. For an existing policy, please provide a summary of the revisions made to the policy.)

The revised University Access Control Policy (3-105.2) streamlines responsibilities, strengthens reporting timelines, and modernizes procedures for managing physical and electronic access. Oversight now falls under the Associate Vice President for Utilities and Engineering Services (UES) and the Associate Vice President of Public Safety. The policy clarifies that the Department of Security manages electronic access systems, while Facilities and Business Operations (FBO) oversees physical key control, ensuring unified governance under UES and Public Safety.

Reporting and return procedures have been tightened. Building liaisons must report lost or stolen keys to the Work Control Center and file a UCF Police Department report within the same business day. Keys must be returned to supervisors by the end of an employee's last shift, to the building liaison within one business day, and to the WCC within two business days. UCF ID cards must also be collected upon separation. Unauthorized locks or padlocks will now be removed at departmental expense, and "PIN-only" access requires explicit written approval from the Director of Security Management.

The definitions section has been expanded for precision and consistency, adding new terms such as Floor Master Key, Housekeeping Key, and Master Key as a general category. The definition of Critical Infrastructure now includes both physical and virtual networks. The approval matrix was restructured to include additional oversight roles—such as the Directors of Security Management and Facilities Maintenance, and the AVPs of UES and Public Safety—and adds clearer approval paths for specialized areas like housing, telecom, and floor-level access.

Procedures for access requests, key issuance, and audits have been strengthened. Departments must now maintain internal approval processes for electronic access, and the former "Contractor Key Request Letter" has been replaced with a Vendor Key Request Form. Electronic access audits are required annually, with supervisors prohibited from using access records for attendance tracking. Non-residents can no longer be issued residential keys, and vendors who lose keys are financially responsible for rekeying all affected areas.

Finally, "key control and recordkeeping" responsibilities have been centralized under FBO, which now maintains all electronic records, oversees approved key control boxes with two-factor authentication, and performs regular audits. Exemptions and rekeying approvals require authorization from both the AVP of UES and the VP of Public Safety.

Stakeholders included in the Review Process: (Provide a list of departments involved in the review/revision process.)

Utilities and Engineering and Public Safety

Stakeholder feedback must also be requested from the Faculty Senate and the College Policy Liaisons. By checking the boxes below, you are confirming that feedback from these groups was requested, received, and considered in the draft policy.

☒ College Policy Liaisons ☒ Faculty Senate

Regulatory Requirements (if applicable)**:** (Provide information on regulatory requirements pertaining to the policy, including specific statute or regulation number.)

N/A

Presenters: (Provide the name(s), position title(s), and email address(s) for all individuals who will be presenting the policy to the university's Policies and Procedures Committee.)

Duane Siemen, Associate Vice President for Utilities and Engineering Services and Chief Engineer. Steven Freund, Senior Director, Security Management

Draft-University Access Control

Policy Number 3-105.~~1~~ 2
Responsible Authority ~~Assistant Vice President for Facilities Operations;~~ Senior Associate Vice President ~~for Facilities Operations~~Utilities~~Public Safety~~ and Engineering Services and Chief Engineer ~~Chief of Police~~
Senior. Director, Security Management
Initiating Authority ~~Sr.~~ Acting ~~Vice President for Administration & Finance & CFO~~ , and Vice President for ~~Administrative~~ Operations
Effective Date ~~5/6/2022~~
Date of Origin 12/7/2017

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 vendors~~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~~ vendors 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, including all key control boxes storing University keys, is administered by University Operations.~~Facilities and& Business Operations (FBO). F&BO).~~

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

administration of the university approved ~~Electronic~~ electronic ~~Access~~ access ~~Control~~ control ~~System~~ 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 a Single Keyed Different (SKD) key. ~~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 if electronic card access is not available. The university will not issue physical keys to students unless they are actively employed by the university and in pay status or reside in on-campus housing and require a physical key to their residence. With the approval of the dean, director, or chair, students who experience no more than a one-semester gap in university employment may retain their access during that gap. Student access must be coordinated through their department and may only include electronic card access or access to required keys in a university-approved key control box. Individuals without an active employee or student affiliation will not receive electronic card or physical key access and must be escorted and supervised while in secure locations. All access must be in accordance with university policy 3-122 Campus Safety and Health.

University Operations ~~FBO. 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 and building liaison if an access card or physical key is lost or stolen. The building liaison must notify ~~FO~~ the University Operations ~~FBO~~ Work Control Center (WCC) of all lost physical keys and must immediately, but within the same business day, file a report with the UCF Police Department for all lost~~Lost~~ or stolen SKD~~Building Sub-Master, Building Master~~ or master~~, submaster, master, grandmaster, or great-grandmaster~~ keys. SKD ~~, submaster, master, grandmaster~~or master~~, or great-grandmasterGGM~~ keys will not be replaced until a report has been filed with the UCF Police Department. The building liaison must immediately, but within the same business day, remove all~~Upon separation from the university, electronic~~ access from and notify the Department of Security ~~if an access card is lost or stolen~~of a lost or stolen access card.~~will be terminated, and employees must return all university physical keys to their University Access Control Representative (UACR).~~

Upon separation from the university, electronic access must be terminated and UCF ID card collected (in accordance with U~~u~~niversity P~~p~~olicy 3-132 UCF Identification Cards and Badges) by the end of the employee's last shift, and employees must return all university physical keys to their immediate supervisor, who must then return them to their building liaison within one business day. The building liaison must then return the~~se~~ key(s) to ~~FO~~the WCC within two business days of receiving the key(s). The building liaison is responsible for properly securing all returned keys in their possession between collecting them and returning them to the WCC. Keys that are not returned will be considered lost~~,~~ and associated rekeying and key issuance charges will be assessed to the department. Individuals who do not return physical keys when requested or upon separation will be responsible for costs associated with rekeying and issuing new keys.

The Department of Security, in conjunction with Planning, Design, and Construction (PDC), 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~~meets all Department of Security requirements and published construction standards. Other~~,~~ existing access control systems may continue to be used for existing doors but cannot be expanded, repaired, 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 in writing by the Department of Security. Unapproved systems will be removed at the installing department's expense.

All doors with electronic access control must also be on the university physical key system and be accessible only by an SKD key~~the Building Master or GGM~~, unless approved by the ~~director~~ Sr. Director of Security Management~~, AVP of FO,~~ and the ~~director~~ Director of Environmental Health & Safety (EH&S) (for academic and research laboratories containing hazardous items).

Padlocks used to secure gates, roof hatches, or other openings that might need to be passed through by an individual or vehicle, must be supplied and keyed by the University Lock Shop. Padlocks will be keyed according to this policy, and any locks that are not keyed to the master key system must be approved by the Sr. Director, Security Management.

Doors that~~which~~ protect critical infrastructure, as identified by the Department of Security, ~~FBO~~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. PIN-only access is only permitted with the written approval of the Sr. Director, Security Management.~~—~~

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 University~~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 and will result in the department performing the work to incur the cost of necessary repairs and/or returning the door and lock system to an approved state.

Individual Responsibilities

Individuals~~Whenever possible, individuals~~ should access buildings and rooms using electronic access where available. Physical keys~~key~~ should only be used in emergency situations or if electronic access control is not installed. 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 as soon as possible. If the individual is unable to secure the space, they should contact the WCC for assistance.

The building liaison~~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 building liaison. ~~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.~~The Sr. Director, Security Management must provide written approval to the requesting department for any door locks installed on campus that are not part of the university's key system. Locks installed without written approval~~an approved form~~ will be removed and replaced with an approved lock at the department's expense. Key requests that are not covered by this policy must be approved by the Sr. Director, Security Management.

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 access to others without proper, prior authorization
- Admitting unauthorized person(s) into a building
- Failing to immediately return a physical key when requested by University Operations ~~FBOFO~~, the Department of Security, Human Resources, the building liaison, supervisor~~UACR~~, or upon leaving employment with the university
- Failure to return surrendered keys in the required timeframe
- Losing a physical key or electronic access card due to negligence
- Failing to immediately report missing physical keys or electronic access cards
- Failing to return a ~~Building Master or GGM~~ key to a key control box within the allotted timeframe ~~12-hour curfew~~
- Attempting unauthorized access to a space without proper authorization
- Accessing a space without successfully completing the required training
- Using electronic access control records for supervisors to track employee attendance

Violations of this policy may result in the loss of electronic card access privileges, ~~and/or~~ physical key issuance, and/or 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~~ Vendors who violate this policy may lose access to a space, the campus, or the university may sever the business relationship.

DEFINITIONS

Building Liaison. Facilitates the exchange of facilities, accessibility, and safety-related information between the building's occupants and Department of Security, Department of Emergency Management, UCF Police Department, Facilities and Business Operations, Student Accessibility Services, and UCF IT.

Building Master Key. A physical key that accesses ~~any lockset, with the exception of mechanical/electrical, telecom, and roof locks,~~all building-occupant accessible doors, with the exception of doors keyed to an SKD key, in a specific building.

Building Submaster~~Sub-Master~~ Key. A physical key that accesses multiple locations ~~a lockset in an area/suite~~ within a specific building. Includes suite master keys. ~~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.

Floor Master Key. A physical key that accesses all building occupant-accessible doors on a single floor of a building, except for doors keyed to an SKD key.

Grand Master (GM) or Zone Master Key. A physical key that can provide access to multiple buildings.

~~**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** **Housekeeping** **Key**. A physical key that accesses janitorial housekeeping rooms.~~

Leased/Managed Space Key Representative. A non-UCF employee occupying a UCF owned space

via a lease or management 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~~Electronic Access Card~~ that is assigned to a specific employee, or that can be accessed by that employee in a ~~physical~~ key control~~security~~ box, to be used by another individual.

Master Key. A physical key that can operate a set of several locks. Types of master keys can include grand master keys, zone master keys, building master keys, floor master keys, and building submaster keys.

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.

Single Keyed Different (SKD) Key. A physical key that is not keyed to the university's master key system. Often used for high security areas or on doors with electronic access control.

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~~period.

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.

Unauthorized Person(s). An individual without a legitimate university-related reason to be present in an access-controlled space.

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~~various levels of approval. The approval paths for each access type are as follows:

Access Type	Building Liaison ~~UACR~~	Dean, ~~-~~ Director, ~~-~~Chair	~~Lock Shop or Facilities Asset Management~~ Sr. Director, Security Management *	Director, ~~FO~~ Facilities Maintenance	~~IT Telecom~~Special Approval	AVP of ~~FO~~UES~~,~~ or ~~Chief of Police~~AVP of Public Safety
~~Great Grand Master (GGM)~~	~~X~~	~~X~~	~~X~~	~~X~~	-	~~X~~
Grand Master (GM) or Zone~~Building~~ Master	X	X	X	X		X
Building ~~Sub-~~ Master ~~(Suite)~~	X	X	X	X	-	-
Building Submaster (including Floor Master)	X	X	X	-	-	-
Academic, Research, or Administrative Room/Space	X	X	~~X~~	-	-	-
Regulated Research Room/Space	X	X			Information Security Office	
Housing Space	X	X	X	X	AVP Campus Housing	
Electrical, Mechanical, Utility, Roof, Housekeeping, or Elevator Machine ~~-~~Room	X	X	X	X	-	-
Roof	~~X~~	~~X~~	X	X	-	-
Janitor	~~X~~	~~X~~	X	X	-	-
Telecom	X	X	X	X	~~X~~ Assoc. Dir., Telecom	-

SKD Keys	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.

Prior to accessing spaces on campus, keyholders (physical or electronic) are responsible for verifying that all applicable, required training on the EH&S Workplace Safety Training Matrix has been successfully completed. Certificate(s) of completion must be included with the associated key request.

Vendors will not receive access to any occupied residential building. Vendor access to residential buildings either must be escorted if the building is occupied or may be unescorted (upon approval) if the building is completely unoccupied.

2. Access Requests

a. Electronic Access Requests

Departments mustwill 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 building liaisonUACR, and departmental approvers.

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

All building liaisonsUACRs 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 FBOF&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 on the University's masteraccessible using a university key systemGGM, 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 mustwill submit a request to their building liaisonUACR, who mustwill submit it through the online key request system, along with the appropriate documentation. Residents in campus housing buildings must submit In order to be issued access to a GGM, Electrical, or Mechanical key requests through, the Department of Housingperson for whom the key is being requested must complete EHS training course 690, Electrical and Residence Life (DHRL), which if approved, will be fulfilled by the Lock ShopMechanical Room Safety at UCF, and submit the certificate of completion to his or her UACR.

Contractors Vendors requiring keys must submit a Key Request Letter to the university contact managing the project, who mustwill then forwardVendor Key Request form to FOthe appropriate UACR for approval, in accordance with the chart below. FOThe UACR may grant access to

contractors vendors on either an annual or project-specific basis. Access may not be granted for longer than twelve months. one calendar year. Approved Key Request LettersVendor Key Request forms will be kept on file in FO. the Facilities Resource Center (FRC).

Contractor	Annual Physical Key Request	Project-specific Physical Key Request	Physical Key Request Type
Elevator, Fire Alarm, Security	X	-	Grand/Zone Master GGM
All OtherUtilities, 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

Building liaisonsUACRs must perform an annual review audit of all individuals with electronic access to their buildings and rooms and updateupdate, as necessary. The results of the review audit, including the date the audit was performed, buildings/rooms audited, and cardholders who had access removed, should be maintained by the unitunit, and provided to the Department of Security upon request.

Authorized University OperationsFBOF&BO employees will be given electronic access to all the areas in which they perform their job functions. Authorized UCF IT employees will be given access to any telecommunications rooms with electronic access. University Operations FBO and UCF IT will designateOnce an individual who will be responsibleis approved for conducting audits of their employees withGGM access to buildings and rooms on campus and verify thatthrough the online key request system, corresponding GGM electronic card access is in accordance with their job responsibilities. If a cardholder's access cannot be justified, the individual performing the review shall report the access to the cardholder's chain of commandwill 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 will 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.

Building liaisonsUACRs must revoke an individual's access to buildings immediately upon termination, by the end of their final shift. 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. ~~Access control records must not be used by supervisors~~Supervisors must not use access control records to track employee attendance.

4. Electronic Access Control Hardware Installation and Maintenance

Requests to add electronic access control hardware to existing buildings and rooms must~~shall~~ be initiated by contacting the Department of Security. ~~Upon approval, the requesting department must~~will submit a Minor Project request through Facilities Planning, Design, & ~~Construction (PDC). FP&C).~~ Existing classrooms, teaching and research laboratories, conference rooms, rooms containing a key control box, 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 PDC. ~~FP&C.~~ The unit or department installing the electronic access control hardware shall be financially responsible for installation.

All new construction must~~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 key control boxes, rooms with high-value items, ~~and~~ secure storage areas, and other areas deemed necessary by the Department of Security. All access control installations must~~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~~Key Request Form~~ must be completed~~filled out~~ for each person requesting keys. Only room/space~~For suites with more than 24 doors, a maximum of two Building Sub-Master (Suite)~~ keys will be issued to individuals. All other~~; any additional requested Suite~~ keys will~~must~~ be housed in a key control~~security~~ box. Building entry~~Additional Suite~~ keys ~~will~~ may be issued to occupants of buildings if the building does not have electronic access control installed on its exterior doors. Non-resident access to physical keys to residential buildings and spaces will be managed through key control boxes. Physical keys to residential spaces will not be issued to non-residents~~are only allowed~~ for any reason~~suites with 24 doors or less~~.

The key must be picked up in person Monday through Friday 8:00 a.m. – 5:00 p.m. at the Facilities & Business Operations reception desk~~FRC~~, located in building~~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.~~The individual to whom the key is issued, or the building liaison, must pick up the key. Keys not picked up within 30 days will be returned to the Lock Shop, and a new key request~~Key Request Form~~ must be submitted. Keys are billed (if applicable) when the Lock Shop processes the key request~~Key Request Form~~; therefore, additional charges will be incurred for new key requests. Arrangements to pick up keys after hours or on weekends must be coordinated in advance through University Operations~~FBO~~.

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

Access to GGM and Building Master keys in are issued to key controlsecurity boxes will be via an electronic key request.a work order, not individuals. Approved individuals may check out a GGM or Building Master key from a designated key controlsecurity box during their work shift. Anyone authorized to use a GGM, or Building Master key must exercise extreme vigilance in protecting it at all timesalways protecting it.. Employees and contractors vendors who have been approved to use a GGM or Building Master key will be assigned a key controlsecurity box location from which to access the appropriate key. Keys from key control boxes not must 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.

ForWhen contractors vendors requiring report to the FRC to obtain keys, they will be required to show a picture ID,and approvedFRC will retrieve the appropriate key(s) for key accessthe contractor. For satellite campuses, an electronic access card will be provided to each approved individual listed on the Key Request LetterVendor Key Request form for the duration of the project that will allow the individual access to the key controlsecurity box in building 16Aat the satellite campus. If a project's timeline is extended, the contractor may request extended access by updating the original Key Request LetterVendor Key Request form and electronically submitting through the UCF representativeit to University OperationsFBO. However, if the initial access period has already expired, or if it's going to extend past a one year, the contractor vendor must submit a new Key Request LetterVendor Key Request form. Vendors that lose a key will be financially responsible for rekeying all spaces that the lost key opens, as well as covering the cost of all keys that must be re-issued because of the rekey.

All Building Master, Electrical, Mechanical, Roof, and Great Grand Master keys checked out from a key control box must be returned to the FRC within the designated curfewimmediately once the key is no longer needed, and not to exceed a period of 12 hours. An exception may be made if the employee's shift extends beyond 12 hours of checkout.

Employees within the UCF Public Safety may bePolice Department who are authorized by the Chief of PoliceAssociate Vice President of Public Safety to retain access past the designated curfew and may take them off remove a GGM key from campus if necessary.

All keys remain the property of the University of Central Florida and or authorized to override the 12-hour curfew must be surrendered upon requesthave 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 supervisorUACR, who then must return the key(s) to the building liaison within one business day. The building liaison mustwill

~~complete the~~a Key Return Form~~,~~initiate the electronic key return process and submit ~~it, along with~~ the key to the ~~FBO reception desk~~WCC in building 16A Monday through Friday from 8:00 a.m. – 5:00 p.m. within two business days. Arrangements to return keys after hours or on weekends must be coordinated in advance through ~~FO~~the WCC.~~, 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 or when an employee moves to a different UCF department shall~~may~~ result in departmental charges or charges to the employee~~,~~ if a rekey of the space is deemed necessary by the AVP of ~~FO~~ UES, VP of Administrative Operations, or the ~~Chief of Police~~AVP of Public Safety. A receipt will be issued for each key ~~returned, and~~returned and will be considered the official record of the key return. Keys may not be transferred from one individual to another~~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.

The university may conduct key audits of leased/managed facilities at any time, and if the university believes key control to have been compromised, it may mandate a facility rekey at the leaseholder or management company's expense.

When an area requires additional security or confidentiality due to legal, compliance, or safety-related reasons, a Request for Exemption from the University Key System to rekey a door off of the campus master key system~~GGM~~ must be submitted to and approved by the AVP of ~~FO~~ UES and the ~~Chief of Police~~AVP of Public Safety. 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 Public Safety~~Police Department~~ for emergency purposes.

8. Physical Key Control

~~With the exception of~~Except for ~~the~~ UCF Public Safety~~Police Department~~, physical key control is facilitated ~~through the use of~~using a ~~physical~~ key control box approved by the AVP of ~~FO~~UES. Shared access to a key must only be facilitated through an approved~~. Physical~~ key control box. Key control boxes that are not approved by the AVP of ~~FO~~ UES 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 ~~FO~~University Operations~~FBOF&BO~~, through a ~~chargeable~~ work order. ~~FO~~ University Operations ~~FBO~~ will determine the appropriate box to be installed. The department will also be responsible for permitting fees, material and installation charges, ongoing administrative fees, licenses, and maintenance.

~~With the exception of~~ Except for UCF Public Safety, all key control boxes will be managed by ~~FO~~University Operations ~~FBO~~. Key control boxes shall be configured for two-factor authentication such as requiring both card and PIN.

~~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 ~~FBO reception desk~~WCC when replacement key is picked up.~~FRC.~~ Keys not returned to the ~~FBO reception desk~~WCC~~FRC~~ will be billed as lost.

10. Key Records and Audits

- ~~The Lock Shop will maintain individual key records~~University Operations~~FBO~~ will maintain electronic records of all keys issued~~.~~.
- ~~Departmental key reports are available to the building liaisonUACR in the University Key System.~~ Building liaisons may request reports of keyholders for their buildings and rooms by submitting a work order.
- ~~All university keys must be returned to the building liaisonUACR when an employee separates from the university, transfers departments, changes room assignments, or upon request from the Lock Shop.~~
- ~~FO~~ University Operations ~~FBO~~FRC will retain copies of all active ~~contractor Key Request Letters~~Vendor Key Request forms and will notify the appropriate UCF representative when a ~~contractor's~~ vendor's ~~Key Request Letter~~key authorization is one week from expiration.
- ~~FO~~ University Operations ~~FBO~~ will periodically perform physical inventories of keys, including departmental key control boxes. Departments will be charged for missing keys and any required rekeying.~~.~~
- Building liaisons will be responsible for auditing electronic card access in their building(s).

RELATED INFORMATION

Building Liaison Policy 3-101
Campus Safety and Health Policy (3-122)
UCF Identification Cards and Badges Policy (3-132)
Key Forms
Minor Project Request Form

CONTACTS

Department of Security
Environmental Health & Safety (EH&S)
~~Facilities Operations (FO)~~
University Operations ~~Facilities and Business Operations (FBO)~~

~~Department of Security~~

~~Key Forms~~
~~Minor Project Request Form~~

History: 3-105, 12/7/2017; 3-105.1 5/6/2022