	FGCU POLICY 3.035	**Responsible Unit**: Physical Plant
	Lock and Key	

A. POLICY STATEMENT

To establish the security of University facilities, Physical Plant manages the University keying systems which includes controlling the production, storage, and issuance of keys; the replacement or re-keying of lock cylinders; the acquisition of new keying systems; the maintenance of accurate electronic and hardcopy key records; and the cataloging of and adherence to key system authorizations. All locks and keys must be approved by the Physical Plant Director, or designee.

B. REASON FOR POLICY

This Policy is to inform the University community of requirements to obtain and maintain keys so to preserve the security of University buildings and their contents while ensuring reasonable usability of campus facilities.

C. APPLICABILITY AND/OR ACCOUNTABILITY

This Policy requires each college, department, or office (hereinafter "Unit") to develop and enforce a key return policy. Units are responsible for costs to secure areas compromised as a result of lost, stolen, or unreturned keys. University Housing facilities are not included under this Policy. Nonetheless, employees within the Office of Housing and Residence Life are to comply with this Policy for their general University key and card access.

D. DEFINITION OF TERMS

1. *Building Access Card (also known as a "proximity card" or "prox card"*): Provides access to the exterior of University buildings and selected labs in academic buildings.

2. *Building Master Key*: Provides access to all spaces within an individual building.

3. *Building Sub-Master Key*: Provides access to a group of rooms within a Unit.

4. *Computer Aided Dispatch (CAD) Event Report:* University Police Department generated incident report used to conduct a security assessment for each lost, stolen, or missing key.

5. *Duo Proximity Access Card or Duo Prox Card*: Provides access to both proximity readers, such as building exterior readers and labs, and magnetic card access, which

allows access to academic classrooms on campus. The employee Eagle ID is a Duo Proximity Access Card. All general classrooms are included in "faculty level" access.

6. *Grand Master Key*: Provides total access to all buildings within a particular system on campus.

7. *Individual Room Key (also known as an "operator level key")*: Provides access to a room or office within an individual building.

8. *Key Custodian*: Unit-designated employee responsible for managing all key transactions and conducting annual key inventories.

9. *Key Recipient:* The employee or contractor who is issued a key to a University facility.

10. *Key Record*: All documentation for key transactions, such as key agreements, key transfers, and contractor key agreements. A Key Record remains active until the key has been returned or a CAD Event Report has been received for the lost or stolen key. Key Records are used to provide key inventory lists to each Unit for annual audits. Work Management Center is responsible for entering the data, generating agreements, and maintaining files. The Key Custodian is responsible for returning key(s) to Work Management Center when not in use and for submitting key transfer forms, etc.

11. *Magnetic Card*: Provides access to rooms with Magnetic Card access such as an academic classroom, but is unable to access proximity readers on campus. Eagle ID cards only have the magnetic function and require encoded access in order for the Eagle ID to function.

12. *Suite Key*: Provides access to an individual office as well as the main suite door, supply room, or various shared spaces within a Unit.

13. *Unit:* Any University college, department, or office that requires key or card access to University buildings or rooms for its employees.

14. *UPD:* University Police Department.

15. *Work Management Center (WMC)*: The Unit of Physical Plant responsible for, among other things, accepting and monitoring work requests related to lock and key access and key distribution.

E. PROCEDURES

All lock and key work shall be done by the Physical Plant Lock and Key shop. UPD and Physical Plant maintenance personnel must have unrestricted access to all campus areas for safety, security, and health reasons. This access is provided through the establishment and maintenance of a master keying system. Any request for access must be submitted in writing,

with justification, to the Physical Plant Director.

1. Key Custodians

    a. Key Custodians are appointed by either the Vice President of a division or the Unit head, in writing, to WMC.

    b. Key Custodians will act as liaison between WMC and building occupants within their Unit.

    c. WMC will provide periodic training to Key Custodians.

    d. Authorized signature of the Key Custodian is submitted to WMC as updates occur on the Key Custodian Authorization form.

    e. The Key Custodians are required to attend annual training sessions.

2. Requesting Keys

    All lock and key requests require an approved form to be submitted in advance. Signed lock and key request forms may be delivered by interoffice mail, hand, fax, or scanned and emailed to WMC and have a printed name as well as an approved signature.

    a. Identify the building(s) and room(s) for which access is required. WMC will determine the key requirements necessary to provide such access.

    b. Submit a Key and/or Access Request form through the Key Custodian with appropriate information, and signature.

    c. WMC will review the information provided to confirm the level of lock and key access requested.

3. Unit Key Authorization

    a. Notwithstanding, approval for the issuance of a Grand Master Key shall be done by the Vice President for Administrative Services and Finance or the Director of Public Safety, and this key shall only be issued to University security and maintenance personnel. Notwithstanding, the issuance of a Building Master Key is restricted to employees authorized by the Physical Plant Director and Vice President of the division in which the employee is employed.

    b. Approval for the issuance of a physical key or electronic access to a Key Recipient, to any University room or building shall be by the division Vice President or Unit head of the Unit responsible for the use of that building or room. Issuance of a physical key or electronic access to any multi-unit buildings require approval from all affected

division Vice Presidents or Unit heads or their respective designees.

c. The key will be fabricated when Unit approval is received. The Key Custodian and the authorized Key Recipient will be notified when the key is ready for pick up at WMC.

d. The authorized Key Recipient must personally pick up and sign for any key issued by WMC.

e. Keys will not be issued to anyone but the authorized Key Recipient. University or state-issued identification is required.

f. Lock and key requests will usually be completed in three (3) to seven (7) business days.

g. All keys must be picked up from WMC within thirty (30) days or the request is void and a new request must be completed before a key can be issued.

4. Contractors, Consultants, Vendors, and other Non-University Personnel "Contractor": (Checkout for longer than one (1) business day)

   a. For construction and renovation projects, keys will be issued only for the duration of a building project and arrangements must be made through the Associate Director of Maintenance and Operations.

   b. Contractor must sign the contractor key agreement.

   c. The Contractor's authorized Key Recipient must present a state-issued identification card and personally checkout each key from the Associate Director of Maintenance and Operations. Keys will not be issued to anyone not designated as the Contractor's authorized Key Recipient.

   d. New contractor key agreements must be obtained for each key change out during the project.

   e. The Contractors are responsible for the safekeeping and use of the key(s).

5. Contractors, Consultants, Vendors, and University Personnel "Contractor": (Checkout for one (1) business day only)

   a. Contractors may temporarily checkout keys from WMC.

   b. Contractors must present a state-issued identification card or Eagle ID.

   c. A temporary key checkout agreement must be signed by the Contractor.

d. The contractor's authorized Key Recipient assumes responsibility for the safekeeping of the key and its use.

e. When leaving a campus area or building, all doors must be secured.

f. The key must remain in the possession of the Contractor at all times.

g. All keys are due back at the end of the business day.

h. The contractor assumes financial responsibility for all lock changes and re-keying required due to unreturned keys.

6. Non-Chargeable Key Issues

   a. A Key Recipient will not be charged for the issuance of a key in the following instances:

      1) The issuance of a replacement key as a result of the re-keying for reasons other than the employee's loss of the key;

      2) The issuance of a replacement key to replace a worn key. The employee must return worn key to WMC prior to issuance of the replacement key;

      3) The issuance of a replacement key as a result of the re-keying of a building or group of rooms for reasons not as a result of the employee's loss of key. The Key Recipient must return key to his or her Unit's Key Custodian prior to being issued a new key; or

      4) Any key exchange required due to administrative moves, construction, or building renovations. The Key Recipient must return the key to their Unit's Key Custodian prior to being issued a new key.

7. Chargeable Key Issues

   A Unit may be charged for a key replacement in the following instances:

   a. When a Unit makes a request for lock changes for operational changes not related to Unit moves. The costs of re-keying in these instances will be billed or charged back to the Unit making the request.

   b. When lock changes are required to maintain building security following lost or stolen key incidents. Lost or stolen keys will not be replaced until a CAD Event Report has been filed with UPD. The CAD Event Report will contain the details necessary to determine responsibility for the lost, stolen, or missing key. Charges will be assessed

to the Unit. The University may charge the individual after a review of the CAD Event Report by the Physical Plant Director.

c. In the event a key must be replaced because of the loss or theft of a key, the replacement of the lost or stolen key will be charged to the Unit employing the Key Recipient who is determined to have lost the key or has had the key stolen. That Key Recipient may also be charged for the replacement key(s) by their Unit.

d. When a replacement key is issued after the loss of a key and does not require the replacement of locks, cores, and keys, the cost of the replacement key may be charged to the Unit. The Unit may charge the Key Recipient.

e. The failure to return an assigned key upon request will result in a charge to the Key Recipient's Unit. The Unit may charge the Key Recipient.

f. The Physical Plant Lock and Key Shop will provide an estimate for re-keying as a result of a chargeable key issue. Examples of the estimated cost of common key replacement:

Office Key (one (1) door)	$90.00
Suite Key (average ten (10) doors)	$900.00
Building Sub-Master Key (based on access to twenty (20) doors)	$1,800.00
Building Master Key (issued only upon Vice President approval)	$4,000.00 or more

g. All estimated expenses (combinate and install new core, update records, and issue new key) necessary to re-secure University property are contingent on the number of areas affected. A greater number of affected areas will result in a higher cost to the Unit. The labor and material costs may be subject to change, based on market conditions.

h. When lock changes are requested due to reorganization or Unit changes, the Unit will be charged based on the number of cores and keys involved and the Unit will receive a detailed estimate prior to commencement of work.

i. Unauthorized door locks are prohibited and if found will be removed and the costs for the removal will be charged to the responsible Unit.

8. Returning Keys

a. Key Recipient

Return all keys to the Key Custodian or WMC before separation from the University or transfer within the University. Keys are not to be turned over to anyone else

because as individuals, the student, faculty, or staff will be held responsible for the return of every key issued to the Key Recipient.

b. Contractor

All keys issued to a Contractor must be returned to WMC at the completion of the project.

9. Lost, Stolen, Un-returned, and Broken Keys

a. Keys Not Returned

1) It is the responsibility of the Key Custodian to make best efforts to secure keys from a Key Recipient when that person is separating from the University or transferring Units.

2) If efforts fail to obtain the key, it will be considered lost and the Key Recipient will be assessed for any charges related to the loss.

b. Lost Keys

1) Lost keys must immediately be reported to UPD and WMC.

2) A CAD Event Report must be filed by the Key Recipient or Unit detailing the circumstances of the loss, including, but not limited to, where the key was believed to be lost by the Key Recipient and how long it has been considered lost.

3) A Key and/or Access Card Request form must be submitted to WMC for the lock change and replacement key. Each Unit is responsible for the total cost of lock changes and new keys to secure areas compromised by a lost key.

4) A lost key will not be replaced until a CAD Event Report has been filed with UPD. The recommended security risk from the Unit will be reviewed by WMC and UPD will determine if reissue of the key is appropriate or if replacement of locks, cores, and keys is needed.

c. Stolen Keys

1) A stolen key must immediately be reported to the appropriate Key Custodian, UPD, and WMC.

2) A copy of the CAD Event Report must be filed by the Key Recipient with WMC.

3) A new key request must be initiated for replacement keys.

4) A Key and/or Access Card Request form must be submitted to WMC for the lock change and replacement keys. Each Unit is responsible for the total cost of lock changes and new keys to secure areas compromised by a stolen key.

5) A stolen key will not be replaced until a CAD Event Report has been filed with UPD. The recommended security risk from the Unit will be reviewed by WMC and UPD will determine if reissue of the key is appropriate or if replacement of locks, cores, and keys is needed.

d. Broken or Damaged Keys

1) If a key is broken or otherwise damaged, the pieces must be returned to WMC.

2) If a key is broken off in a lock or is malfunctioning, the Key Custodian will immediately notify WMC to repair or replace the lock.

3) A new key will be issued after damage verification. There is no charge for the replacement key when replacing a broken or damaged key.

10. Inventory

a. Each Unit is responsible for keys issued within its area(s), for both the security of University buildings and its contents, as well as the cost to re-secure the area should security become compromised by the loss of a key.

b. Key Custodians will maintain accurate records of lock and key requests, key transfers, and key returns to track key inventory changes within their Unit.

c. WMC will routinely review and check outstanding temporary key issues.

d. WMC will provide each Key Custodian with an annual key inventory list, per an agreed upon schedule. The inventory list will include each key issued, by person, with associated financial liability should any keys be compromised.

11. Audit

a. Annually, each Unit will be provided a key inventory list assigned to the Unit.

b. The Unit head will confirm that the designated Key Custodian physically checks the accuracy of the annual key inventory list for all keys issued within that Unit, according to the agreed upon annual inventory schedule.

1) Each Key Recipient with a confirmed key assignment is required to have a current key agreement on file.

2) Updated key agreements will be provided to Key Recipients required to carry a Unit key.

3) A key that is no longer needed or authorized for use will be returned by the Key Custodian to WMC and the Key Record will be removed from inventory.

12. Electronic Access System

An alternate to physical key access is available for many areas on campus via an electronic access control system. Physical Plant is responsible for the purchase, installation, and maintenance of campus-wide electronic access control systems which uses the Eagle ID to allow access.

a. Hard keys for electronically controlled doors will only be issued to UPD and Physical Plant Maintenance. All building perimeter doors will be secured by either key or centralized access control system components. All requests for exceptions to this rule must be submitted in writing to the Director of Public Safety and the Physical Plant Director.

b. Key Custodians will request electronic access for faculty, staff, and students via email to WMC.

c. The propping open of electronically controlled or monitored doors is not permitted except with prior notification and approval of UPD.

d. Tampering with or attempting to bypass security on an electronically controlled or monitored door in any way including, but not limited to, key bypass, propping, taping, or disabling is prohibited and may be subject to disciplinary action consistent with University regulations and policies.

e. If an Eagle ID is damaged or inoperable, it is the responsibility of the Key Custodian to investigate all access problems and refer the Key Recipient to the Eagle ID Card Office to obtain a new Eagle ID. WMC will program the new Eagle ID.

f. Lost or stolen Eagle ID should immediately be reported to WMC so that access can be disabled to University property.

13. Violations

Alleged violations of this Policy will be addressed through the appropriate University regulation, policy, or collective bargaining agreement. The University may also refer alleged or suspected violations of applicable law to appropriate law enforcement agencies.

Authority
BOG Regulation 1.001, University Board of Trustees Powers and Duties

History of Policy
New 07/03/12; Amended 07/31/19

APPROVED

*s/Michael V. Martin	July 31, 2019
Michael V. Martin, President	Date