



<b>Policy Title:</b>	University Keys
<b>Policy Number:</b>	UNIV- 436
<b>Revision Date:</b>	October 2019
<b>Policies Superseded:</b>	FINA-1150; FINA 450
<b>Policy Management Area(s):</b>	Facilities

**SUMMARY:**

This policy sets forth the conditions under which Facilities Planning and Management provides locksmith services and maintains a record of all lock and key schedule systems on campus. Additionally, this policy provides direction to departments/supervisors as to what action(s) should be taken to ensure that University keys and any other University property issued to employees are properly distributed and maintained, and that any such keys and/or property are returned upon an employee’s separation from University employment. Departments/units should develop and maintain a system to issue, monitor and retrieve keys and other University-owned equipment supplied to employees.

**POLICY:**

I. Issuance/Maintenance of Keys

All University keys are the property of Coastal Carolina University. The director of Facilities Planning and Management or their designee is responsible for regulating the issuance, control, accounting and return of all keys issued for all University facilities. The Lock and Key Control section of the Repairs and Renovations division of Facilities Planning and Management has day-to-day responsibility for implementing the Lock and Key Control measures. To ensure that University facilities, equipment and the campus community are secure, it is expected that departments/supervisors will properly issue and monitor keys distributed to employees.

A. Lock and Key Control

The director of Facilities Planning and Management has the authorization to initiate detailed internal procedures needed to implement this policy. The department is responsible for designing and developing the schematics for the master key lock system. This includes maintaining the master key lock system records, making new keys, establishing combinations for lock cores, furnishing all of the required forms used in the procedures, and providing reports requested by University units.

## B. Approving Authorities

The president, senior vice presidents, other vice presidents, deans, directors, and other authorized officials may approve key requests for employees within their departments. The responsibility for keys once issued rests with the department/unit official(s) that authorized the issue. Responsibility begins upon delivery of the key to the requestor from Lock and Key Control and ends when the department/unit returns the key to Lock and Key Control. It is the responsibility of the department/unit authorized official(s) to secure all keys from personnel (faculty, staff or students) terminated from the University or transferring to a different department. The department/unit is responsible for keys not returned or lost by unit personnel and for the cost of re-establishing the security of areas affected by the loss of keys. Such costs will vary, depending on the extent of the University facilities affected by the loss. This could range from re-establishing security of one door to re-establishing security of the entire campus. Department/unit heads may authorize additional keys for personnel who have documented needs for extra keys.

1. Departments/supervisors must retain a log of employees receiving/returning keys. Any key that has been checked out from an authorized central location should be returned at the end of the workday.
2. It is recommended that extra/duplicate keys be kept in a locked cabinet and coded appropriately with the code being filed separately for security purposes. The University does not allow duplication of University keys by outside sources.
3. Employees must safeguard keys issued to them. In the event a key is lost or stolen, it is the employee's responsibility to notify their supervisor immediately. Loss and/or failure to report stolen keys may be subject to disciplinary action up to and including dismissal.
4. Departments/supervisors are responsible for notifying Facilities Planning and Management and/or Public Safety immediately if keys are lost or stolen.

## C. Key Recipients' Responsibilities

Employees who accept the responsibility for University keys are authorized to use the keys only to gain access to their work stations during normal working hours, for overtime work, or as approved by the department/unit head. Using the assigned key to gain entrance to other University offices or facilities is strictly prohibited. Employees are responsible for immediately reporting lost keys to the Lock and Key Control unit in Facilities Planning and Management. All keys which are not utilized by the department/unit or which are obsolete must be returned to Lock and Key Control for disposal. Persons issued keys are responsible for their safekeeping. Do NOT loan, transfer, borrow or duplicate any key(s) without proper authority and documentation of Lock and Key Control.

## D. Master Key System and Master Key System Identification

Master keys will be issued to individuals having a continuing need for a master key. The request must have the appropriate authorization and justification. All costs incurred to re-establish the security of areas affected by the loss of a master key will be borne by the department/unit requesting the issuance of said key. Any employee that accepts custody of a master key will be required to sign a statement acknowledging their responsibility for the key's uses and care. All master key distribution requires the approval of the senior vice president of finance and administration/chief financial officer. Master key system identification will be maintained in a highly secure area by Lock and Key Control. Knowledge of the location will be limited to those University officials on a "need to know" basis, and to those who are authorized by the president or the senior vice president of finance and administration/chief financial officer.

#### E. Locks Removed from the Master Key System

Circumstances may infrequently occur that result in specific (high risk/high security) areas within the University needing to be removed from the master key system. In order to remove a lock from the master key system, the senior vice president for finance and administration/chief financial officer must submit a letter to Lock and Key Control documenting the necessity for removal. A copy of the request, the documentation, and a summary of the action taken must be sent to the director of Facilities Planning and Management, to the director of Facilities Operations, to the University fire marshal, and to the Department of Public Safety. Lock and Key Control will be responsible for ensuring that keys to those areas removed from the master key system are available to the fire marshal for placement in appropriate Knox boxes. Duplicate or department/unit keys will not be provided. In the event that the Department of Public Safety is unable to contact the individuals having access to these specific areas and forcible entry is necessary, the department/unit will be responsible for the cost of repairs.

Barring an emergency situation, accessing these areas without the consent of a key holder is prohibited.

High-risk/high security areas may include:

1. Volatile storage.
2. Office of Student Accounts.
3. Vaults where money or valuables are stored.
4. Lock and Key Control.
5. University Public Safety.
6. Audio-visual.
7. Vital records.
8. Pharmacies or drug storage.

#### F. Lost or Stolen Keys

1. Employees are responsible for immediately reporting lost or stolen key(s) to their department/supervisor.

2. Departments/supervisors are responsible for notifying Lock and Key Control, Facilities Planning and Management, and/or Public Safety immediately if key(s) are lost or stolen.
3. The department/unit is responsible for keys not returned or lost by unit personnel and for the cost of re-establishing the security of areas affected by the loss of keys. Such costs will vary, depending on the extent of the University facilities affected by the loss. This could range from re-establishing security of one door to reestablishing security of the entire campus.

#### G. Key Issue

1. Once the need for an employee to have a key is determined and approved, the authorizing department/unit must submit a work request via the online work request system at [myschoolbuilding.com](http://myschoolbuilding.com). The work request is valid when submitted by an approved requestor. In addition, a completed key agreement (Lock and Key Control form), available on the University forms page, must be submitted to the Facilities Planning and Management department.
2. While no undergraduate student workers will be issued key(s), graduate assistants can be authorized to be a key holder. As in I.G.1. above, the authorizing department/unit must submit a work request via the online work request system at [myschoolbuilding.com](http://myschoolbuilding.com). The work request is valid when submitted by an approved requestor. The key will be issued to the professor associated with the graduate student. The professor is responsible for issuing and monitoring the key.
3. It is the responsibility of Lock and Key Control to:
  - a. Verify the approving signatures.
  - b. Cut key(s) as stated on work request.
  - c. Complete all records needed prior to issuance of the key(s); once completed, return the work request to the Facilities Management office.
  - d. Deliver the key to the requesting department/unit and obtain signature of receipt.
4. Upon separation from employment, an employee is required to immediately return all key(s) in his or her possession. Failure to do so may result in deduction from wages for any unreturned items. The University has the right to pursue criminal prosecution as appropriate.
5. When an employee transfers to another department or separates from employment, departments/supervisors should collect all key(s) issued to that employee and return them, along with a completed key return form (available on the University forms page), to Lock and Key Control as soon as possible, but no later than five (5) to seven (7) days from the date of separation or transfer of said employee.