41.01.01.C0.02 Building Access and Key Control

Revised: March 4, 2024
Next Scheduled Review: March 4, 2029
Revision History

Procedure Summary

This procedure outlines access control for university-controlled buildings, rooms, and facilities. It also establishes a process to secure the campus environment and ensure accountability. Student access to resident housing is managed by Islander Housing and not covered by this procedure.

Definitions

Access Card: An employee's identification card that manages access through the authorization and revocation of rights to controlled areas. An access card may also be other access media types such as a cellular telephone, cellular telephone application, RFID chip card, or i-Button RFID chip device.

Contractors or Contract Employees: Any person employed by a business other than Texas A&M University (TAMU-CC), who has been contracted to operate a business or service function of the university.

Off-Hours: Outside the normal open hours of university buildings. Generally, normal open hours are Monday through Friday from 7:00 am until 11:00 pm.

Procedure

1. GENERAL

1.1. All keys issued are to be considered state property and should be protected with the same considerations. The TAMU-CC key and access system must be protected as any other expensive state property. Stringent key and access control accomplishes this. Careful consideration should be given to every key and card access authorization request.

1.2. The University Police Department (UPD) at TAMU-CC is responsible for

managing and coordinating the design of the university's key and access control system. The Security Services Office (UPD-SSO) is the area within the UPD that manages the campus wide access control system including all SandDollar$ swipe card access and door key requests.

1.3. University keys are TAMU-CC property and may be recovered at any time by UPD.

1.4. The UPD is responsible for approving the fabrication of all TAMU-CC campus keys. University keys will not be duplicated without a written request on file.

1.5. Unauthorized fabrication, duplication, possession, or use of university keys is a violation of this procedure.

1.6. The UPD will maintain all records of keys to university facilities, including the names of individuals to whom keys are issued and dates of issue, return, and loss as applicable.

1.7. The UPD will only grant an individual access to their own office/suite. Exceptions may be made based on extenuating circumstances, at the discretion of the President, a vice president, the Chief of Police, or the responding UPD officer and upon proper identification of the party requesting access and documentation as to the reason why access is needed.

1.8. Employees found in violation of this procedure may be subject to disciplinary action up to and including termination of employment.

2. KEY HOLDER RESPONSIBILITIES

2.1. Key holders shall not prop or otherwise hold doors or windows open or leave them unlocked during hours when the facility is normally closed. If for some reason a door cannot be locked with an issued key, the UPD must be contacted.

2.2. Key holders shall not unlock buildings or rooms for others unless the individual has a valid, verifiable reason and proper identification for access, or is known by the key holder to have legitimate need for access to the room or building. Suspicious persons should be reported to the UPD immediately.

3. CONTRACTOR KEY AND ACCESS REQUIREMENTS

3.1. Contractors and other non-university users found in possession of unauthorized university keys will have their keys confiscated, and the individual(s) may be removed from university property. A criminal trespass warning may be issued, and criminal charges may be filed.

3.2. Keys required by contractors or other non-university users to access areas on campus to conduct their work must be requested by the project contact person and authorized by the UPD-SSO. University keys issued to contractors must be returned at the end of each business day to the UPD for storage unless the contractor has been authorized by the Vice President for Finance and Administration (or their designee), the Chief of Police, or the requesting dean/director/department head (or designee) to retain the issued keys for the duration of the project.

3.3. The project contact person will provide the UPD with the names of contractors authorized to receive designated keys. Contractors authorized to receive keys must show photo identification to sign out and return keys to the UPD. Information as to who is issued keys and when they are signed out and returned will be recorded by the UPD-SSO, the Parking Division Customer Service desk, the Police Communications Center Officer, or other UPD designee.

3.4. All costs of key recovery or re-keying related to unreturned keys will be the responsibility of the contractor and/or their company to which the keys were issued, and final payment for services provided will not be made until all issued keys are returned or payment for lost keys is made.

4. KEY AND ACCESS CARD REQUESTS

4.1. Deans, directors, department heads, or their designees can only request keys and access to a building, suite, or office for which they have direct control. At no time will keys or access be issued to an individual without authorization of the controlling dean, director, department head, or their designee.

4.2. All key requests will be reviewed by the UPD to ensure proper security protocols are followed. The types of master keys are listed below. At no time will a Master Key or Sub-Master Key be issued if the issuance of such a key is determined to compromise the safety and security of the campus community.

4.2.1. Campus Great Grand Master Keys can access all university doors, and their issuance must be approved in writing by the President or the Vice President for Finance and Administration.

4.2.2. Master Keys can access specific university buildings, and their issuance must be approved by the President, Vice President for Finance and Administration, the Chief of Police, or the appropriate dean, director, department head, or their designee.

4.2.3. Sub-Master Keys can access to a group of locks within a specific building, and their issuance must be approved by a vice president, or

the appropriate dean, director, department head, or their designee.

4.3. An office or individual door key must be approved by the key holder's (employee's) dean, director, department head, or their designee.

4.4. Access cards can provide access to buildings and facilities 24/7. A request for off-hours card access may be made by the President, Vice President for Finance and Administration, dean, director, department head, or their designee. UPD may determine that granting access poses a risk to the safety and security of the campus community and/or the university's facilities and may recommend denial of the request.

4.5. Requesting issuance of card access or a physical key for access to a building, room, or facility must be submitted using the request process as managed by UPD.

4.6. All key request forms must be filled out completely and approved by the appropriate dean, director, department head, or their designee.

4.7. It is the responsibility of each dean, director, department head, or their designee to monitor and control all keys and card access issued for spaces under their direct control.

4.8. All completed key and access requests will be submitted to, and processed by, the UPD-SSO.

4.9. A UPD-SSO representative will verify all sections of the key or card access request form are completed and accurate prior to issuance of any key or card access. Any incomplete requests will be sent back to the requesting dean, director, department head, or their designee for correction or clarification. Notice of approved keys and card access requests will be issued by the UPD in a timely manner.

4.10. Keys can only be picked up by the person for whom the keys are approved.

4.11. Keys not picked up within 15 calendar days of notice of approval will be restocked and a new key request must be completed and submitted in order to pick up the key.

4.12. Requests for keys or access may not be made for any building, area, or department that is under the supervision of another dean, director, or department head. An exception to this requires authorization from the President, Vice President for Finance and Administration, dean, director, or department head who has control over the building, area, or department.

4.13. All key requests are kept on file in accordance with the university's records

retention policy.

5. RETURNING A KEY OR ACCESS CARD

5.1. The individual who was issued the key(s) and/or access card is responsible for ensuring the key(s) and/or access card is returned upon separation from the university. In the case of involuntary termination, Human Resources collects the key(s) and returns them to the employee's supervisor. The keys are to be returned to the UPD-SSO. Giving keys to a faculty member, staff member, dean/director, department head, administrative assistant, or other person will not clear a key record.

5.2. All key(s) must be returned to UPD before proper clearance may be granted. The university will use all means available to collect and/or charge for lost or unreturned key(s).

5.3. If key(s) are not returned, a police report must be filed by the original requesting dean, director, department head, or their designee.

5.4. A receipt indicating payment for lost key(s) must be presented to the UPD at the time of termination if the faculty member, staff member, department head, director, or their designee does not have possession of the actual key.

5.5. If the employee is also a student, diplomas, grades, and/or transcripts may be held until the key(s) are returned or costs of key recovery or re-keying are paid.

6. REPLACING A LOST KEY OR ACCESS CARD

6.1. Keys and access cards are issued to a specific individual, and that individual is responsible and personally held accountable for the use/misuse or loss of said keys and cards.

6.2. All lost keys must be reported within 24 hours to the appropriate dean, director, department head, or their designee and the UPD. Individuals are responsible for initiating the process of replacing their key(s) within five (5) business days from the date of loss.

6.3. Access cards with UPD-applied building access should be reported lost immediately to the appropriate dean, director, department head, or their designee and the UPD.

6.4. Information about stolen or lost keys and access cards should include, if known:

(a) Where the key or card was stolen from or lost;

(b) Date when the key or card was stolen or lost;

(c) Key number and room(s) the key opened; and

(d) Buildings and/or rooms that the access card opened.

6.5. Payment for the stolen or lost key(s) will be made to the University Business Office. There may be a fee for any lost or stolen access cards which will be charged to the individual to whom the access cards were issued and handled by SandDollar$ Services.

6.6. The department originally authorizing issuance of the key(s), at its own discretion, may choose to take responsibility for the cost of replacing the key(s). The department is under no obligation to do so.

6.7. If the lock core must be changed for security reasons as determined by the Chief of Police or President or their designee, the actual cost of re-keying will be determined by Administrative Operations, and the cost will be charged to the individual to whom the key(s) were issued. The department originally authorizing the key(s), at its own discretion, may choose to take responsibility for the cost of the re-keying. The department is under no obligation to do so.

6.8. Prior to issuance of a replacement key, a payment receipt for stolen or lost key(s), a new key request approved by the appropriate dean, director, department head or their designee, and a copy of the UPD lost key report must be submitted to the UPD. Replacement access cards are handled by SandDollar$ Services.

7. ACCESS TERMINATION

7.1. Access for faculty and staff will expire upon separation from the university.

7.2. Access for graduate students and other student employees will have a two-year expiration date assigned to the access unless otherwise specified on the request.

7.3. All card access will be removed on the last day worked upon separation of a faculty member, staff member, or student from the university.

Related Statutes, Policies, or Requirements

System Policy *41.01, Real Property*
System Regulation *41.01.01, Real Property*
University Rule *41.01.01.C0.01, Use of University Facilities*

University Procedure *41.01.01.C0.03, Management of Buildings, Grounds, and Other Improvements*

This procedure supersedes:

- *41.05.02.C1.01, Building Access*

Appendix

Card Access and Key Request Form
Lost or Stolen Key Information

Contact Office

Contact for clarification and interpretation:	University Police Department 361.825.4242