



STANDARD OPERATING PROCEDURE

SOP #	1034	Owner	Sr. Director of Maintenance
Revision #	3	Revision Date	2024-06-06
ACCESS CONTROL, NON-RESIDENTIAL (UNT Policy 11.005)			

PURPOSE

Proper management of access control systems, keys, and key systems are paramount in the ensuring that the University's students, faculty, staff, and assets are protected.

SCOPE

The purpose of this Standard Operating Procedure is to provide processes which assist in ensuring proper access control and key management procedures.

PREREQUISITES

Policy for Access Control, section 11.005

PROCEDURE

(1) Key Authorizer Process

- A. A Dean, AVP, Vice President or Chancellor may appoint a Key Authorizer using the *Addition or Revision of Authorizer* form. An individual may be appointed as a Key Authorizer for a specifically defined area within a building or buildings.
- B. Once appointed, a Key Authorizer will be added to the master database of Key Authorizers maintained by FACO.
- C. Employees will be removed from the Key Authorizers master database upon termination of employment from the University, or if removed as a Key Authorizer by their *Approving Authority*. The *Approving Authority* is responsible for notifying FACO of any required changes to the Key Authorizer master database.
- D. Once advised of any required changes, FACO will update the database accordingly.

(2) Key Authorization

- A. Key Authorizer may approve key requests for rooms in their defined area of authority by signing Key Request Forms on the appropriate signature block and forwarding to the FACO office.
- B. Key Authorizers will prohibit the exchanging or loaning of keys.
- C. Key Authorizers, Building Representatives, and Deans are responsible for building hours and card swipe authorization.

(3) Access Control

- A. Upon receipt of a properly authorized and completed Key Request Form, FACO is authorized to prepare and issue the requested keys.
- B. FACO has the responsibility for maintaining records of all locks, key codes, key holders, key authorizers as well as all key transactions (issuances, replacements, deletions, etc.)
- C. FACO will issue keys as quickly as possible based upon current workload and product availability.
- D. Upon receiving the key/electronic access request, FACO will

release/grant access to the approved key(s) to the approved key/card holder at the office during normal business hours.

(4) Key Holder Responsibilities

- A. Key/Card Holders are responsible for picking up their approved keys at FACO, and/or bringing the electronic access card FACO for programming during normal business hours.
- B. The individual key holder named on the key request must be present with photo ID to receive the key. FACO will not release a key to anyone other than the named key holder unless special arrangements are made with the Key Authorizer.
- C. Key Holders shall not exchange, duplicate, or loan their keys, nor shall they accept custody of university provided keys not issued to them through this process.
- D. Inappropriate use of keys by key holders may result in the immediate surrendering of the keys to the appropriate Key Authorizer or directly to FACO.
- E. Upon exiting the Organization or transfer to a different area within the organization, all unnecessary keys must be returned to FACO to ensure they are removed from the key inventory system.
- F. Key holders must take reasonable measures to protect their keys from theft, loss, or unauthorized use.

(5) Lost Keys

- A. Key Holder must report lost keys to FACO immediately so that appropriate measures can be taken to maintain building or property security.
- B. Replacement keys may be issued if deemed appropriate by FACO and the appropriate Key Authorizer.
- C. Security for areas compromised by the loss of a key(s) by a Key Holder shall be evaluated by the Facilities Department, in consultation with Campus Police and Risk Management, to determine whether there is a need for rekeying the compromised areas.
 - a. Recommendations for rekeying will be forwarded to the VP for Finance and Administration for final approval and funding source determination for the cost of rekeying affected areas.

(6) Return of Keys Upon Termination

- A. Upon termination of employment, all keys issued to a key holder must be returned to the University.
 - a. Keys must be returned to the authorizing department, the Key Authorizer, or to FACO.
- B. When terminating employees fail to return assigned keys, FACO will undertake a risk assessment to determine whether rekeying doors and/or locks is necessary to restore the level of security needed.
 - a. If the assessment reveals that rekeying or other actions are necessary, the AVP for Facilities will be advised so that the information may be forwarded to the UNT General Counsel's Office for review and determination of appropriate action up to and including litigation for collection of damages.

- C. When keys are not returned by terminating employees, FACO will notify Human Resources for inclusion in the terminating employee’s personnel record.
- D. Keys that have been lost by the terminating employee will be handled according to the “Lost Keys” provisions stated above.

(7) Departmentally Controlled Keys

- A. To assist with the issuance of keys to Faculty as they receive/turn in keys at the beginning/end of each semester, an optional process is available to academic departments, which expedites the process.
 - a. Key Box Authorizer must be approved by the AVP of Facilities or its designee to receive a departmentally controlled key.
 - b. FACO creates keys for each participating department and issues them to the Department through their Key Authorizer.
 - c. The Key Authorizer is responsible for issuing, tracking, receiving returned keys, and re-issuing keys as needed using a tracking sheet provided by FACO.
 - d. The Key Authorizer is responsible for storing keys in a Facilities approved storage unit/box.
 - e. The Key Authorizer is responsible for each key that is not assigned and issued to an individual.
 - f. FACO will be responsible for auditing issuance records for each department to ensure that proper key control is occurring.
 - g. In the event that proper key control is not occurring, the issue will be discussed with appropriate leadership.
 - h. If a key is lost or cannot be accounted for see section (5) Lost Keys above.

REFERENCES

Reference	Description	Location
Policy 11.005	Policy for Access Control	https://policy.unt.edu/policy/11-005
Form	Addition or Revision of Authorizer	
Form	Key Request	

DEFINITIONS

Term	Description / Definition
FACO	Facilities Access Control Office
Key Authorizer	Individual approved to authorize the issuance of keys or electronic access to specific areas.
Key Holder	Individual approved to the issuance of keys or electronic access to specific areas.