



UT System Administration Policy Library -- Policy INT145 **Key Control Policy**

Responsible Officer: Director of Police
Sponsoring Office: Office of the Director of Police
Effective Date: August 1, 2006
Last Reviewed: May 22, 2010
Next Scheduled Review: August 31, 2010
Errors or changes to: policyoffice@utsystem.edu

CONTENTS

Policy Statement

Rationale

Scope

Website Address For This Policy

Related Policies, Requirements Or Standards

Contacts

Definitions

Responsibilities

Procedures

Forms Tools/Online Processes

Appendix

POLICY STATEMENT

To provide electronic card key and metal key access to offices of UT System Administration employees located in the Austin complex.

RATIONALE

To control security and access to the UT System Administration complex. To maintain control of the number of keys issued to employees. It is the responsibility of the employee to maintain the security of all issued keys.

SCOPE

All offices of UT System Administration

WEBSITE ADDRESS FOR THIS POLICY

<http://www.utsystem.edu/policy/policies/int145.html>

RELATED STATUTES, POLICIES, REQUIREMENTS OR STANDARDS

None

CONTACTS

If you have any questions about UT System Administration Policy INT 145, *Key Control Policy*, contact the following offices:

Subject	Office Name	Telephone Number	Email/URL
	Office of the Director of Police	512-499-4680	http://www.utsystem.edu/pol/

DEFINITIONS

None

RESPONSIBILITIES

Director of Police and Office of the Director of Police

- Approves issuance of building master keys, sub-master keys, or electronic card keys which allow full access to System Administration Facilities.
- Approves issuance of temporary metal keys or electronic card keys to outside vendors and contractors who require after hour access to System Administration Facilities.
- Approves type of access allowed for all employees, vendors, and contractors issued electronic card keys.
- Issues a memorandum addressed to UT Austin Locks & Keys Department.
- Maintains records of all metal keys issued for access to system administration facilities.
- Issues electronic card keys.
- Maintains records of access cards for facilities with a computerized magnetic locking system.
- Acts promptly upon reports of the loss or theft of metal keys or card keys and will notify department head of reported losses.
- Maintains a secure electronic database to support an electronic card key system for System Administration facilities.

Key Recipient

- Submits a memorandum or e-mail request to their department head requesting a metal key.
- Assumes full responsibility for the security and proper use of both metal keys and electronic card keys.

- Reports the loss or theft of any key within 24 hours to the Office of Director of Police, their immediate supervisor, and their Department head.
- Returns the issued key(s), in person, to the Office of Employee Services upon their retirement or termination of employment.
- If an employee relocates to another office area within the U. T. System Administration complex, the issued metal key must be returned to the Office of the Director of Police.

Department

- Submits written requests for re-keying of locks.
- Controls entry and exit to the department's office area during the period of afterhours use.
- Submits request and justification for issuance of electronic card key for extended afterhours access.

Department Head

- Authorizes issuance of metal keys to System Administration employee and forwards original employee request to the Office of the Department of Police.
- Approves requests for individual office or room metal key(s) or electronic card keys for employees.
- Ensures keys are returned when the employee no longer needs the key(s) or terminates employment.
- Verifies reports of lost or stolen keys with the Office of the Director of Police within 24 hours of discovery of theft or loss.
- Pays applicable re-keying costs when re-keying is necessary.
- Acts promptly upon reports of the loss or theft of electronic card keys or metal keys.

Vice Chancellor for Administration

- Final approval for the issuance of a building master and/or area sub-master key(s) or electronic card keys allowing full access to System Administration facilities.
- Approves special exceptions for more than one key being issued for a lock.
- Approves special exceptions for locks not being in the master key system.
- Approves fees for lost or stolen keys.
- Final approval for the issuance of temporary metal or electronic card key to outside vendors and contractors who need afterhours access to System Administration facilities.

PROCEDURES

1. Issuance of Keys

1.1 Routine access to locked System Administration facilities or areas within those facilities required for the performance of an employee's assigned duties will be provided through the issuance of an appropriate key for entry.

1.1.1 The Director of Police has immediate responsibility for the issuance of metal keys and for maintaining records of all keys issued for access to System Administration facilities in accordance with procedures approved by the Vice Chancellor for Administration.

1.1.2 The Director of Police has immediate responsibility for issuance of electronic card keys and for maintaining records of the access cards provided for those facilities in which a computerized magnetic locking system has been installed in accordance with procedures approved by the Vice Chancellor for Administration.

1.1.3 Keys may be issued to System Administration employees only upon authorization of a responsible Department head and approved by the Director of Police. Any disputes on the issuance of keys are resolved by the Vice Chancellor for Administration.

1.1.4 Persons to whom metal keys or electronic card keys are issued assume full responsibility for the security and proper use of keys issued to them. Key recipients must agree they:

- a.** may not lend or otherwise permit any type of keys issued to them to be used by any person not authorized;
- b.** may not duplicate or alter the key and may not allow others to do so;
- c.** must report the loss or theft of any key within 24 hours to the Office of Director of Police, their immediate supervisor, and their Department head;
- d.** shall return the issued key(s) to the Office of Employee Services upon their retirement or termination of employment. (Office of Employee Services will not certify clearance forms for individuals terminating employment from System Administration until all keys issued to the employee have been returned.) Keys may not be sent through the U.S. or campus mail; rather, they must be delivered in person. Keys must also be turned in for office relocation

1.1.5 Appropriate fees approved by the Vice Chancellor for Administration will be assessed for damage, loss, or failure to return an assigned key or for

replacement of an assigned key. Additionally, re-keying costs also may be assessed for each lock affected by a lost or unreturned key. Failure by an employee to return a key may result in a financial hold on provision records until such time as the key is returned or the lost key fee is paid and the cost of any required re-keying has been reimbursed by the employee.

1.2 Key Control Procedures

1.2.1 The Vice Chancellor for Administration is the final authority to approve the issuance of a building master and/or area sub-master key(s) or electronic card keys allowing full access to System Administration facilities.

Department heads and Directors are authorized to approve requests for individual office or room key(s) or electronic card keys for employees.

1.2.1.1 When requesting a metal key, a Key Request memorandum or e-mail must be properly approved and submitted to the Director of Police. When issued, the employee must personally go to the U.T. Austin Locks and Key Shop to be issued the key and sign for the key.

1.2.1.2 No more than one key for a particular lock will be issued to an individual. Special exception may be granted upon written approval by the Vice Chancellor for Administration.

1.2.2 The authorizing Department head is responsible for:

- a.** initiating requests for metal keys to be issued to employees in their department;
- b.** maintaining current, accurate records of all metal keys approved by him/her, and adopting procedures to maintain adequate security within the assigned departmental or unit areas;
- c.** ensuring keys are returned when the employee no longer needs the key(s) or terminates employment;
- d.** verifying reports of lost or stolen keys with the Office of the Director of Police within 24 hours of discovery of theft or loss;
- e.** paying applicable re-keying costs when employees lose or do not return issued keys upon termination and re-keying is determined necessary;
- f.** preventing the installation of door locks that have not been approved by the Vice Chancellor for Administration.

1.2.3 The Director of Police is responsible for:

- a.** approving the issuance of building master keys, area sub-master keys, or electronic card keys allowing full access to System Administration Facilities;

- b. approving 24/7 full access or other type of access;
- c. maintaining a keying system that provides security and convenience to departments occupying System Administration facilities;
- d. maintaining current, accurate key control records and issuing reports of keys issued as required;
- e. acting promptly upon reports of the loss or theft of all keys to ensure appropriate investigation and determination of security risks;
- f. maintaining a secure electronic data base to support an electronic card key system for System Administration facilities;
- g. providing individually encoded electronic access card keys that provide access to selected facilities for authorized individuals;
- h. acting promptly upon reports of the loss or theft of electronic card keys to ensure maintenance of facility security.

1.2.4 The Key Recipient is responsible for:

- a. using issued key(s) to gain access only to authorized area(s) to conduct University business and for the safekeeping of all University keys in their possession;
- b. storing keys in a locked storage cabinet or kept in their possession. Filing cabinets, desk drawers, and lockers are not considered to be secure storage areas for University metal keys or electronic access cards.
- c. ensuring the door(s) to a keyed assigned work area is properly locked or otherwise secured at the conclusion of work;
- d. returning issued keys that are no longer needed due to relocation, reassignment or termination of employment;
- e. reporting lost or stolen keys, as prescribed in this policy, within 24 hours of discovery of loss or theft;
- f. paying for replacement of lost keys or keys not returned upon transfer or termination of employment and for possible re-keying required by negligent loss of keys.

2. Lost or Stolen Keys

The loss or theft of keys (metal and electronic card keys) must be reported within 24 hours of discovery of the loss or theft to the Office of Director of Police, the immediate supervisor, and the administrator who originally authorized issuance of the key or card. Individuals issued the lost or stolen key(s) shall be responsible for paying the applicable replacement fees. Replacement metal keys will be issued only after submission of a new key request authorization form and payment of applicable fees. Fees for unreturned keys, including lost and stolen keys, and for replacement of keys or cards, shall be as approved by the Vice Chancellor for Administration.

3. Re-keying

As a general rule, the re-keying of rooms and/or buildings will be required whenever metal keys are lost or stolen if the Director of Police, after analyzing the circumstances associated with the loss or theft, determines that security of the affected facility has been compromised. In such cases the individual to whom the key was issued and/or the Department head that authorized issuance of the key may be held responsible for the costs of the re-keying. Decisions to require re-keying at departmental expense may be appealed to the Vice Chancellor for Administration.

Departments may also unilaterally request re-keying of locks by submitting a written request justifying the requirement for re-keying to the Vice Chancellor for Administration. Re-keying is not considered routine maintenance and the department requesting re-keying normally will be charged for the work.

4. Vendor and Contractor Keys

Temporary metal or electronic card keys may be issued to outside vendors and contractors that need afterhours access to System Administration facilities when no other alternative is available. Such access must be approved by the Director of Police upon submission of a written justified request by the appropriate authorized administrator of the department or office accepting responsibility for supervising use of the temporary keys. Before keys are issued, vendors and contractors will be required to sign an agreement to pay re-keying costs if for any reason they fail to return issued keys. Vendors and contractors must also acknowledge that funds may be retained from payments due the vendor or contractor in order to reimburse the System Administration for costs associated with re-keying the affected area(s).

5. after Hours or Temporary Access

When a department or office requires access to System Administration facilities during periods other than normal working hours, arrangements can be made to have the facility or area opened. The department or office must provide adequate advance written notification to the Office of Director of Police for arrangements to open and close the facility. The department will make arrangements with the Office of the Director of Police to assign an overtime guard to control access to the facility. The department is responsible for providing an account to pay the overtime personnel.

Employees may access the System Complex, including the parking garage, after hours, on weekends, or holidays as long as they possess their employee badge/electronic card key and display it upon request by the guard on duty. For safety reasons, employees shall make contact and inform the System Complex Guard of their presence and upon their departure.

6. Penalty for Unauthorized Key Use

Any person, who knowingly makes, duplicates, possesses, uses, or allows a person not authorized to use keys for entry of System Administration facilities or rooms without the

appropriate authorization will be subject to administrative disciplinary action and may be criminally prosecuted under the laws of the State of Texas.

FORMS AND TOOLS/ONLINE PROCESSES

None

APPENDIX

None

Keywords: key control, keys, key, identification, police, electronic card key, metal key, facilities
