

## General Provisions

Provisions in this policy apply to all non-residential facilities for the Missouri S&T campus. Keys for residential facilities are managed by Residential Life and are not subject to this policy.

All keys are issued by the Missouri S&T Access Control Office and shall remain the property of Missouri S&T.

Each building will have a separate building master key system with as many sub-masters as necessary to accommodate the different departments within.

Access devices are for the individual's use for the purpose of conducting university business and should not be loaned to others at any time.

### Definitions

Access coordinator: a delegate, appointed by a department head, having limited administrative privileges within the electronic access control software.

Access device: a physical key or Miner Card ID (university ID card).

## Access Requests

Faculty, staff, graduate assistants and students may be issued keys or granted electronic access to a university space upon the recommendation of the Chancellor, a vice chancellor, dean, department chair, or department director via an online request. The online request must be filled out and then approved by the department chair/supervisor and all required approvers.

### Required Access Approvals

Level	Description	Approval Chain	Applies to Electronic Access	Applies to Physical Keys
1	Level 1 approvals include access to interior or exterior doors with electronic access. A level 2 (or above) approval is required for all doors where key is the only method of access.	Access Coordinator Associated with Door Access Being Requested	X	
2	Level 2 approvals include access to keyed interior doors for rooms assigned to a department. Level 2 approvals do not include building master keys or exterior keys to a building.	Department Chair or Director ↓ S&T Access Control Office		X

3	<p>Level 3 approvals include master keys to any building or set of buildings.</p> <p>All-door (great grand master) electronic access requires a Level 3 approval.</p>	<p>Department Chair or Director ↓ S&amp;T Access Control Office ↓ Vice Chancellor, Finance and Administration</p>	X	X
---	---	---	---	---

## Process After Access Approval is Received

### For Key Issuance

If all required approvals are obtained, a work order is created and keys are cut. When the keys are ready, the requesting individual or contact person listed on the key request form will be notified that their keys are ready for pick up.

A valid state ID or S&T ID card is required when the key holder picks up the key(s) from the S&T Access Control Office located at 901 Facilities Ave. The key holder must provide a signature for each key issued and agree to the terms of this policy.

Records of all keys issued will be kept on a computerized key inventory system and will be maintained by the S&T Access Control Office except Residential Life who maintain their own tracking system.

### For Electronic Access

#### *To Doors Requiring Level 1 Approval*

The department access coordinator may grant the access privilege. The individual is notified by the access coordinator when the access privilege has been assigned.

#### *To Doors Requiring Level 3 Approval*

If all required approvals are obtained, a work order is created and the access is granted. The individual is notified by the S&T Access Control Office when the access privilege has been assigned.

### Key Issuance Delegation

Departments wishing to retain checkout keys will be required to issue keys through the S&T Key Shop's Key Management Software and must follow all procedures associated with key issuance delegation section of this policy.

### Synchronized Access

Some electronic access is granted through synchronized access, and do not require approval after the initial synchronization is approved. For example, a student listed for a specific academic program may be granted access to a specific set of doors; when students are added or removed from this program, they electronic access is automatically updated. All synchronized access must be initially approved by the access coordinator who is assigned the doors in question.

## Return of Keys

It is the responsibility of the key holder to return all keys to the S&T Access Control Office upon the key holder's:

- Transfer to another department
- Termination of employment
- Change of job assignment that makes it unnecessary for the key holder to have certain keys
- Graduation or ceasing to enroll in classes at S&T

All keys must be accounted for and returned. Department chairs or directors will be notified of key shortages upon return of keys to the S&T Access Control Office. Keys should be returned by the keyholder to the S&T Access Control Office and should not be returned to the keyholder's supervisor.

Upon ending employment with the university and as soon as the S&T Access Control Office is notified of the termination date, employees having physical keys will be contacted by the S&T Access Control Office to request that keys be returned. If keys are not returned prior to the final day of employment, the department of employment will be charged a \$250 lost key fee per key. This fee may be refunded upon return of keys.

Upon graduation or ceasing to enroll in classes, students having physical keys will be contacted by the S&T Access Control Office to request that keys be returned. If keys are not returned within 5 days of graduation or no course enrollment, a \$250 lost key fee per key will be charged to the department which approved the key issuance. This fee may be refunded upon return of keys.

Access for Miner Card IDs will be disabled upon:

- Violation of this policy;
- Ending employment with the university;
- Graduation or ceasing to enroll in classes;

## Lost access device

### Lost Keys

The loss or theft of any key should be reported immediately to the key holder's supervisor, S&T Access Control Office, and the University Police Department. Replacement of lost, misplaced or stolen keys will be made in accordance with procedures for original issue. The dean, director, Director of Design & Construction Management, or Director of Facilities Operations will determine re-keying of locks or space at the individual's or department's expense. For employees, the department of employment will be charged a \$250 lost key fee per key. For students, a \$250 lost key fee per key will be charged to the department which approved the key issuance. This fee may be refunded upon return of keys.

If the lost key was issued to a contractor, a lost key fee will be assessed to the contractor. This fee will be calculated as the cost to re-core any locks(s) controlled by the lost key plus the cost to cut and re-issue any control and/or master key(s) for the core(s) being changed.

### Lost Miner Card ID

The loss or theft of any Miner Card ID should be reported immediately to the individual's supervisor and the Miner Card ID Office. Lost Miner Card IDs will be automatically inactive within 40 minutes of reporting the card as lost to the Miner Card ID office. If the Miner Card ID has been granted access to a high security area, the lost card should be reported to the S&T Access Control Office immediately after it has been reported to the Miner Card ID Office.

## Access Coordinators

Departments are permitted to request partial administration of electronic lock access be granted to a Access Coordinator within the department. This delegation is subject to approval by the Assistant Director of Design & Construction Management. For the doors that an Access Coordinator has been delegated access, software permission may be given to:

- Grant / remove access to manually assigned access levels
- View live event logs
- View history event logs

## Electronic Access Event Logs

Electronic access event log requests should be made to the S&T Access Control Office or to an access coordinator that has privileges to all doors needed in the event log. Logs may be requested by departments for events occurring on doors for spaces that the requesting department is assigned and require department head approval. Logs for events occurring on doors for spaces the requesting department has not been assigned require approval by the department head of the department to which the space is assigned.

## Worn Keys

Individuals holding properly authorized keys may exchange damaged or worn keys at the S&T Access Control Office for free replacement at any time.

## Periodic Audit

A key inventory audit and electronic access privilege audit will be issued by the S&T Access Control Office to each university department annually. It will be the department's responsibility to verify the accuracy of the audit and return the audit to the S&T Access Control Office in a timely manner. An annual audit summary will be distributed to appropriate university Vice Chancellors for review.

## Lock Out Procedure

University Police will provide after-hour emergency access for faculty and staff members who need immediate entry to their assigned workspaces. This space is limited to university assigned

offices and scheduled classrooms and shall not include communal areas, laboratories, athletic areas, libraries or other areas. Faculty and staff should first contact their building/department key coordinator, department chair or dean during normal work hours.

After-hours calls should be directed to University Police at 573-341-4300.

## High Security Areas

For areas requiring high security, electronic access control must be used in lieu of keys. For such areas, Missouri S&T IDs will be the sole method for accessing the area, and keys issuance will be allowed for emergency use only. Use of university key on an electronically controlled door will result in a forced entry alarm. Personnel will be sent to the location to investigate the issue. If it is determined that a key was used to operate the door without cause, the keyholder's department will be charged \$50 for the door forced investigation.

## Keys for Doors Having Electronic Access

Key issuance will be limited for doors which are equipped with electronic access, and the MinerCard ID will be the primary method for unlocking these doors. For doors equipped with electronic access, one key will be issued to each of the following:

- The campus department to which the space is assigned;
- University Police
- Facilities Operations

## Policy Violations

Violations of this policy may result in the loss of privileges. Employees determined to have violated this may be subject to disciplinary action up to and including termination of employment. Violations of this policy include, but are not limited to, the following:

- loaning or transferring an access device to another individual;
- obtaining and issuing an access device without authorization;
- damaging, tampering, vandalizing, altering or modifying University access devices, hardware, locks, or other access mechanisms; This includes the installation of any locking devices or hardware (both electronic and mechanical). Unauthorized devices and hardware will be removed by Facilities Operations and the department or individual responsible for the room will be charged for all costs incurred.
- propping doors open to avoid the use of access devices;
- admitting unauthorized person(s) into the building;
- failing to return an access device when requested by the S&T Access Control Office, University Police, the issuing department, or upon leaving the employment of the University;
- failing to report missing access devices;
- failing to comply with the request and approval provisions set forth in this policy;

- attempting or having any access device duplicated by anyone other than the S&T Access Control Office or Miner Card ID Office. University Police have the authority to confiscate any duplicated access devices;

The re-issuance of keys or access privileges may be permitted after the policy violation has been reviewed by the Assistant Director of Design & Construction Management, Locksmith, and Access Controls Specialist.

DRAFT