

## **Policy Timeline**

Initial Effective Date: July 1, 2019

Frequency of Review: Annual

Date(s) Revised:

## **Policy Overview**

The purpose of the key and card access management policy is to provide reasonable security and privacy to the College community. This policy will provide individuals assigned to use College facilities with the guidance and regulation of the issuance, accounting, control and return of all keys/access cards used to control access to College facilities and/or property.

## **Applies to:** (examples—Faculty, Staff, Students, etc)

All faculty, staff, students, contractors, visitors and persons having and/or requesting access to campus either by key or card access. This policy applies to all locking devices securing College facilities and those individuals authorized to use them.

## **Table of Contents:** (optional; suggested for policies > 8-10 pages)

- I. Purpose
- II. Procedures and Policies
  - 1. Identifying Keys and Keying
  - 2. Issuing Keys
  - 3. Issuing Access Cards
  - 4. Key Holder Responsibilities
  - 5. Returning Keys
  - 6. Non-returned Keys
  - 7. Administration of the Key Management Systems
  - 8. Residential Life, orientation, and special events
- III. Record Keeping
- IV. Lost Key and Access Card Replacement Fees

**Definitions: (optional; suggested for terms that have specialized meaning in the policy)**

<b>Term</b>	<b>Definition</b>
Access Cards	Programmable cards that grant the student, faculty, staff or visitor access to specific areas of the College.
Building Master Key	These keys are only approved and issued by the vice president of operations.
Key Control Authority	Key control authority will be given only by the vice president of operations.
Key Control Manager	The key control manager is the individual(s) responsible for the issuance and control of all access cards, keys, as well as the control and maintenance of the lock cylinders and key holders in the College.
Key Control Data	Key control data is all data relevant to; key issuance, key replacement, specific locations, key holders, card holder groups and access rules, and accountable budget.
Key Control Databases	The computerized key control database is the system which houses key control records (Jenzabar) and creates and implements card access controls (Genetec) for the College. Key requests are generated through (Issuetrak) from mysticop page.
Key Holder	A person to whom an authorized key has been issued.
Key Request Form	The key request form is generated by the person requesting a key, which is done through issuetrak. The key request is then approved by the key control manager.

**Office of Public Safety**

Responsible for campus safety and security. After hour access requests must be approved by the director of public safety or his/her designee.

Children's Parking Garage

Phone: 314.446.7233

The parking and access administrator will be responsible for key distribution and inventory.

Jones Hall 1372

Phone: 314.446.8380

**Office of Facilities**

Responsible for processing work order tickets for key requests from issuetrak.

Phone:314.446.8385

## Procedures

### I. Purpose

1. The purpose of this key and card access management policy is to help protect the life, personal property, and security of College property and facilities and all its occupants.
2. It shall serve as the framework by which all keys and access credentials will be managed, issued, duplicated, stored, controlled, returned, replaced and accounted for by the Key Control Authority.
  - a. The Key Control Authority (KCA) comprises the person, persons, department, or committee that has authority to adopt, administer, and enforce this facility's Key Management Policy.
  - b. This policy shall apply to all keys including those to all space, office equipment, vehicles, padlocks, lockers, safes, etc. owned, operated or controlled by the College.
3. This policy seeks to establish a recorded chain of accountability and access for all credentials, keyholders, and locations.
  - a. Establish a key issuance authority.
  - b. Issue appropriate level keys to individuals.
  - c. Establish authority on all key control policies.
4. This policy seeks to implement a proper key control process and then preserve it by restoring security in a timely manner whenever key control has been threatened or compromised.

### II. Policies and Procedures

1. Identifying Keys and Keying
  - a. All keys should only be marked with an identifiable code/number which will indicate what core the keys are to be used on.
  - b. Keys will be marked to indicate level of keying.
2. Issuing Keys- STLCOP Personnel
  - a. All key orders should be properly authorized by an authorized signer, in addition to the keyholder, before issuing.
    - i. Each key can have its own appropriate level of authorization.
      1. Higher level keys may require higher levels of authorization.
  - b. Issue the proper level key to each individual granting only the appropriate level of access.
  - c. Issue keys by need, not desire.
  - d. Require signature(s) on keyholder agreement:
    - i. Signature of keyholder
  - e. Signature of authorizer
  - f. Require photo ID
  - g. Keys shall be issued by duration of need, not by term of employment.

- h. GM keys issued to employees will be stored in the key lock box in facilities and or public safety.
- i. Keys must be personally picked up, not mailed.
- j. Individuals may be issued only one copy of each key.
- k. Keys may not be duplicated or issued except through the KSA or authorized facility locksmith. The key authority will approve all keys through the work order system issuetrak.

### 3. Issuing Keys and Access Cards- Contractors

- a. Contractors under long term contracts for the College may receive STLCOP ID access cards (ie, Coca Cola, Midwest Elevator etc.)
- b. Contractors under temporary project based contracts will have contractor access cards checked out from the key boxes to them either by facilities or public safety.
- c. All key(s) and or access cards should be properly authorized by an authorized signer, in addition to the keyholder, before issuing.
  - i. Each key can have its own appropriate level of authorization.
    - 1. Higher level keys may require higher levels of authorization.
- d. Issue the proper level key to each individual granting only the appropriate level of access.
  - i. An email by a higher level authorizer will be needed.
- e. Issue keys by need, not desire.
- f. Require signature(s) on keyholder agreement:
  - i. Signature of keyholder
- g. Signature of authorizer
- h. Require photo ID
- i. Keys shall be issued by duration of need, not by term of employment/contract.
- j. Signature required by keyholder and authorizer.
- k. Keys must be personally picked up, not mailed.
- l. Individuals may be issued only one copy of each key.
- m. Keys may not be duplicated or issued except through the KSA or authorized facility locksmith.
- n. Keys/access cards will be tracked, depending on the level of key, by the Tile product, and the KeyWin 5 system.
- o. Shift keys or rings shall be returned at the end of every work shift
- p. Shift key rings shall be sealed and tamper evident.

### 4. Issuing Access Cards

- a. All new faculty and staff access will be requested by the Office of Human Resources. Specific access for that position and or employee will be requested from their immediate supervisor.
- b. All new student access will be requested from Office of Student Affairs in conjunction with the Office of Enrollment Services.

- c. Any replacement access card will be requested by the student, faculty or staff. One replacement access card will be given free of charge, any access card replacement thereafter will be a \$20.00 charge to their account.

5. Key and Access Card Holder Responsibilities

- a. All students, faculty and staff are responsible for maintaining building security. A key holder is responsible for all keys issued to them. College issued keys and access cards are the property of the St. Louis College of Pharmacy. The duplication or possession of any unauthorized College key is a violation of this College policy.
- b. The holder of keys to any College facility assumes responsibility for the safekeeping of the key and access card and its use. It's understood that the key and access card is only to be used by the holder and that they will not make it available to anyone else. Should a loss occur due to any circumstance, the department, office and or holder will be responsible for the financial impacts of re-keying and replacing internal cores of an area or facility. (see IV. Lost Key and Access Card Replacement Fees)
- c. In an effort to minimize loss or misuse of keys, all key holders are strongly encouraged to leave College keys in a secure location during non-working periods.
  - i. Employees will NOT loan or transfer their keys to any other individual.
  - ii. Students, faculty and staff shall not unlock a building or room for another individual unless the individual is known by them to have a legitimate need to enter. These requests will be referred to the Office of Public Safety.
  - iii. Authorized access card holders are not allowed to let anyone into a building after business hours under any circumstances except for public safety personnel if required for an emergency.
  - iv. Keys will be returned in to the parking and access administrator when an employee terminates or transfers within the College.
  - v. Doors to unoccupied rooms are to be locked when not in use.
  - vi. Outside doors are to be locked after normal business hours.
  - vii. Enter access requests through the Events Management System (EMS) prior to the date for approval. (<https://ems.stlcp.edu/emswwebapp/>)

6. Returning Keys-Higher Level Authorized Keys

- a. All keys shall be returned to the public safety or facilities lock box after completion of the staff members shift.
  - i. The lock boxes are located in the public safety base station in the Children's Parking Garage and facilities area in South Residence Hall.
- b. Found keys must be turned into the Office of Public Safety.

7. Returning Keys- Termination, Retirement, or Separation from the College

- a. Upon termination, retirement, or separation of an individual from the College all keys, parking access cards, and college id's must be turned into the responsible supervisor then to parking and access administrator.
- b. If an employee changes offices or departments within the College keys should be returned to the parking and access administrator.
- c. All changes regarding key holders should be reported to the Key Control Manager to update the key control database.
- d. If a key is lost or not returned upon termination, separation, or retirement the lock maybe changed and a charge to the student account or a deduction from the former employee's last paycheck will be made. The vice president of college operations has the authority to determine if a lock(s) need to be re-keyed to maintain security.

8. Residential Life, Orientation and Special Events

- a. Office of Student Affairs-Residential Life will be responsible for the distribution and collection for all dormitory cored keys. Residential Life will be responsible for the implementation of policies and procedures for the students living in both the South and North Residence Halls. It should be noted that the minimal acceptable loss of keys from the residence hall is 10 percent or less. Any greater loss will require core swaps for the entire residence hall. The key control authority will dictate further actions for any loss greater than the 10 percent. (see Student Affairs-Resident Hall key procedures)
- b. Office of Student Affairs will be responsible for the distribution and collection for all dormitory cored keys to perspective and or accepted students and parents for the purpose of overnight stays in both the South and North Residence Halls.
- c. Office of Student Affairs will be responsible for the distribution and collection for all dormitory cored keys for any program hosted or sponsored by that office.
- d. VP of operations and events management will be responsible for the distribution and collection of any College cored key to classrooms, conference rooms and both the South, North Residence Halls and any other space on campus.

III. Record Keeping and Inventory Audits

The purpose is to maintain a secure system and an accurate database for the computerized inventory control system of keys issued and returned, and to control unauthorized entry.

- a. All record keeping will be done by the parking and access administrator through two forms, excel documentation and through the College's electronic system jenzabar.
- b. The Office of Facilities will conduct a periodic audit of all facilities personnel issued keys
- c. The Office of Public Safety will conduct random audits on both the facilities and public safety lock boxes.
- d. The director of public safety will conduct monthly audits of the DEA safe and control core keys.

- e. Random audits of access card holder groups and doors will be conducted by the parking and access administrator in the College's access control system.

**IV. Lost Key and Access Card Replacement Fees**

- a. Replacement fees will be charged to the department the individual is assigned. The department or office has the option to pass the charge on to the person the replaced key was issued to for payment.
- b. If a person, office or department believes that extenuating circumstances exist and a fee is unjustified an appeal can be presented in writing to the key control authority to determine whether or not a replacement fee is required.

Key replacement fees are as follows:

Grand Master	\$50,000.00
Building Master Key (if authorized)	\$10,000.00
Sub-master key	\$100.00 per door/room impacted
Individual Office/Room Key	\$25.00
Access Card	\$20.00
Furniture/Cabinet Key	\$(Market Price)
Mailbox Keys	\$(Market Price)

- c. Broken or worn keys/access cards will be replaced at no charge and will be an exact reproduction of the original. Defective items should be brought to the parking administrator for disposal. A new key request must be completed to replace the defective key.

**Responsibilities**

<b>Position/Office/Department</b>	<b>Responsibility</b>
VP of Operations	Key control authority
Public Safety Director	Oversight of security and integrity of key management systems.
Parking Administrator	Inventory and distribute processed keys.
Office of Facilities	Process all key requests that are made.
Office of Information Technology	Support of the software/hardware of the key management system.

**Resources (required for any resource referred to in the policy)**

## Policy Contacts

Name	Contact Information
Scott Patterson	Director of Public Safety
Eric Knoll	VP of Operations

POLICY APPROVALS			
POC:	<input type="checkbox"/> Approved as to Form	<input type="checkbox"/> Not Approved	
POC Chair Signature:			
Date:			
Policy Sponsor:	<input type="checkbox"/> Approved	<input type="checkbox"/> Not Approved	
Signature:			
Date:			
President:	<input checked="" type="checkbox"/> Approved	<input type="checkbox"/> Not Approved	
Signature:	<i>John D. Lopez</i>		
Date:	5/20/19		
Board of Trustees:	<input type="checkbox"/> Approved	<input type="checkbox"/> Not Approved	<input checked="" type="checkbox"/> Not Applicable
Chair Signature:			
Date:			