**Building Access Protocol**

**1. PURPOSE**

The purpose of this directive is to provide written guidelines that establish the standards for access to University facilities as is called for in the CI Administrative Policy on Access Management and Facility Security, Policy Number FA.40.003.

**2. SCOPE**

This directive covers the requirements of a CI Administrative Policy and as such will apply to all individuals requiring access to University facilities. i.e. Students, Faculty, Administrators, Staff, Contractors, Volunteers, and Events Personnel.

**3. RELATED PROCEDURES, DOCUMENTS AND DEFINITIONS**

## Process Guideline No. Description of Process Guideline

TBD Event Fob Use and Function

10/23/2012 Traka Box Use and Functions

TBD Key/Code Request Process

TBD Key/Code Item Request Instructions

## Document No. Description of Document

FA.40.004 Policy on Access Management and Facility Security

<http://policy.csuci.edu/fa/40/fa-40-004.htm>

DFA AD #10-01 Division of Finance and Administration, Administrative Directive, Access Control, Security and CCTV Systems

<http://www.csuci.edu/vpbfa/vp-business-and-financial-affairs/ad-10-1-access-control-security-cctv-systems>

ICSUAM 8080.0 Information Security Policy, Physical Security

<http://www.calstate.edu/icsuam/sections/8000/8080.0.shtml>

TBD Contractor Construction Key Acknowledgement Letter

## Definitions Description of Definition

TBD N/A

**4. OVERVIEW**

It is the policy of the University that other than during normal working hours all buildings shall be locked in order to maintain the safety of both the buildings and their content. Keys/Cards/Codes are issued for entry to University buildings for the purpose of conducting University business only. Facilities Services (FS), is responsible for providing building access on campus, excluding Student Housing, Auxiliaries, Satellite and Tenant facilities. The primary access control to buildings (both exterior and interior) is provided by several methods; a manual key system utilizing various CI “restricted" keyways to prevent unauthorized key duplication and/or Card Readers/Key Pads actuated by entering a code or swiping a card. All campus door locks (except as noted above) shall be keyed/coded within this system. Working with the building users, the Building Access and Security Systems Control Task Force, chaired by Chief of Police, will determine the appropriate lock for each door. The FS Lock Shop will generate keys and codes based on the Task Force findings. No other sources for keys are authorized. All keys issued remain the property of CI. (Keys to vehicles, cabinets, lockers, and desks are not covered in this policy.) The FS Lock Shop will attempt to furnish such keys upon request but the issuance and control of these keys are the responsibility of the individual University divisions and departments.

The Building Access and Security Systems Control Task Force will determine and publish a list that specifies the level of key/access, i.e. Great Grand Master, Grand Master, Building Master, etc. and the approval authority, i.e. VP, AVP, Director, etc. This list will be used by the FS Work Center to determine approval authority in the Azzier (Web Work) Item Request Module and by the FS Lock Shop for confirmation when issuing keys/codes and programming electronic access.

**Objectives**

1. To achieve maximum security while maintaining reasonable usability of University Facilities.
2. To maintain strict control of the campus key and lock systems including key duplication and distribution.
3. To maintain a recorded chain of accountability for all keys issued.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Level of Keys** | **Approval Authority** | **Issuing entity** |
| 1. | Great Grand Master | VP and/or FS Director | FS Lock Shop |
| 2. | Grand Master | VP and/or FS Director | FS Lock Shop |
| 3. | Building Master | AVP and/or Division Director | FS Lock Shop |
| 4. | Departmental Master | Department Administrator | FS Lock Shop via Building Key Coordinator |
| 5. | Individual Door Key | Department Administrator | FS Lock Shop via Building Key Coordinator |

**5. PROCEDURE**

Note: As each function listed below has numerous individual documented Processes or Procedural Guidelines that provide detailed instructions for users they will not be incorporated here in order to limit the size of this document.

**5.1 Responsibilities:**

**5.1.1 FS Work Center**

The initial starting point for all key and code requests on campus is the Azzier (Web Work) “Item Request” module. Access to this module is controlled by the Azzier system administrator with specific individuals across the campus having been granted access to request keys for their respective departments. The process is automated through Azzier with the request ultimately arriving electronically in the FS Lock Shop. The FS Lock Shop verifies approvals for the request and then generates the key/code requested. A response is sent to the original requestor advising that the key/code is available for pick up at the FS Work Center.

FS Process Guideline: Key/Code Request Process

FS Process Guideline: Key/Code Item Request Instructions

**5.1.2 FS Lock Shop**

1. Responsible for creating and maintaining the University's lock and key system, including schematics, codes, product standards and service equipment.
2. Maintain access to computer-based key management system(s) at the FS Lock Shop. The systems currently in use are; Schlage Site master for physical keys, Schlage Security Management Systems for standalone card/keypad readers, and Cisco CPAM for the new electronic access system.
3. Issue keys with proper-signed authorization forms and maintaining records of same.
4. Maintaining computer database of all keys, locks, and associated building and room numbers that they operate. Maintain database of all master key holders and supply various reports to administrators and key coordinators such as which keys open what doors under their control. Report can be done by key or by room number. Numerous other types of reports can be generated as needed.
5. Audit all master keys/codes as required.
6. Restore physical security in a timely manner whenever key control has been compromised.
7. Help departments set up a key record system if requested to do so.
8. Provide education and training in adherence to the key policy and key issuance at no cost to departments.
9. Develop keying schedules, re-keying and stocking necessary locks, cylinders, key blanks and related hardware.
10. All lock and key work shall be done by or through the FS Lock Shop.
11. Provide the keying schedule for the suppliers of key cylinders for contractors constructing new buildings and renovations.
12. Unauthorized door locks are prohibited and when found will be removed and appropriate charges made to the responsible department.

**5.1.3 Academic Affairs, Associated Students Inc., Divisions and Departmental**

1. It is the responsibility of each AVP or Division Director to appoint a key coordinator(s) that will be accessing the Azzier Item Request module. Each Departmental coordinator would request key(s) via the Azzier Item Request module. (Locks are requested via Azzier, Work Order Request module.
2. Protect keys and codes from loss, theft or unauthorized use. Report lost or stolen keys/codes immediately to the Department Manager and to the Police Department.
3. When notified, recipients will pick up their keys/codes at the FS Work Center.
4. Any re-keying or reprogramming expenses to correct deficiencies in security due to a lost, stolen, misplaced, or un-returned key will be the responsibility of the original requesting Department.
5. AVP’s or Division Directors will be required to authorize building master level keys within their areas of responsibility via Traka Boxes.

**5.1.4** **Key Holders--University Personnel and Students**

1. The holder of a key to any University facility assumes responsibility for the safekeeping of the key/code and its use. When leaving a campus area or building ensure that all doors are secured as they were upon arrival. It is understood the key/code will not be loaned or made available to others.
2. Report lost or stolen keys/codes immediately to the Department Manager and to the Police Department.
3. Prior to separating from the University, all keys must be returned to the FS Work Center.
4. Departments are responsible for having key return on their employee exit checklist and ensuring the keys are returned to the FS Work Center.

**5.1.5 Key Holders - Contractors, Consultants, Vendors, and other Non-University Personnel**

1. Before keys or code may be issued the FS Lock Shop requires a current signed document on company letterhead with the employees name and position, stating he/she is authorized to check out keys on behalf of that company and that the company is assuming financially responsibility for all re-keying required restoring security due to keys lost or not returned. Details of this process for contractors are covered in the General Conditions of each project. The Construction Project Manager will be responsible for submitting the necessary key request via the Azzier Key Request Module start and end date of code, and return of keys.
2. Sample document located at: [G:\OPC\370.Logistical Services\SOP ATTACHMENTS\Contractor Key Ack.docx](file:///G:\OPC\370.Logistical%20Services\SOP%20ATTACHMENTS\Contractor%20Key%20Ack.docx)
3. The letter needs to be signed by an appropriate officer of the contractor's company.
4. Loss of keys may require re-keying or reprogramming of one or more buildings and cost many thousands of dollars.
5. The holder of a key to any University facility assumes responsibility for the safekeeping of the key and its use. When leaving a campus area or building ensure that all doors are secured as they were upon arrival. It is understood the key and/or code will not be loaned or made available to others. Report lost or stolen keys immediately to the Department Manager and to the Police Department or FS.
6. The company’s representative to whom the keys are issued must present picture identification and personally sign for all keys/code.
7. All keys must be returned to the FS Work Center at the completion of project. Written confirmation from the FS Lock Shop is required before final payment is made by Project Manager.
8. At the FS Work Center, for short term daily check-out of keys, the contractor/vendor will follow the above steps with the addition of leaving their Driver’s License as collateral until the keys are returned. This is only for daily check-out.

**5.2 Requesting Keys**

The following steps are in place for all entities on campus for requesting keys/codes.

**5.2.1 Key Authorization for Campus Personnel**

1. Determine what building/rooms access is required. The FS Lock Shop can help determine the level of key/code required to provide such access based on schedules provided by the Building Access and Security Systems Control Task Force. Note: All instructional, professional, and clerical space in the building must be controlled by the requestors department to obtain a master key.
2. Submit a Azzier Item Request with appropriate information and account number through your department’s key coordinator.
3. All key requests require a properly “electronically” signed key Item Request submitted to the FS Lock Shop in advance of the date needed.
4. The FS Lock Shop will match the authorization form with the Item Request and verify proper signature(s). The key(s) will be fabricated and the key coordinator notified the order is ready for pick up at the FS Work Center.
5. All keys are to be picked up and signed for by the end user.
6. The person authorized to carry the key must personally pick up and sign for the key at the FS Work Center. As an authorized signature is required keys/codes will not be issued to a third party. Appropriate picture identification will be required.

**5.2.2 Key Authorization for Consultants, Vendors and Other Non-University Personnel**

1. Department Head submits Azzier Item Request with requesters name, company information, and project manager, length of time keys are needed, areas requiring access, and paying account. FS Lock Shop will determine the level of key/code required to provide such access.
2. The Lock Shop will verify there is a current letter of financial rekeying responsibility from the company on file and that no delinquent keys are outstanding.
3. The FS Lock Shop will match the authorization form with the Item Request and verify proper signature(s). The key(s)/code(s) will be fabricated and the requestor will be notified the order is ready for pick up at the FS Work Center.
4. The person authorized to carry the key must personally pick up and sign for the key at the FS Work Center. As an authorized signature is required keys will not be issued to a third party. Appropriate picture identification will be required.

**5.3 Returning Keys**

**5.3.1 CI students, faculty and staff**

Return all keys to the FS Work Center before separation from university or transferring from your present position. Do not turn keys over to anyone else (such as another person who is assuming your position). You will be held responsible for all keys issued to you. The FS Work Center will coordinate with the FS Lock Shop to ensure all keys and fobs are returned. The FS Lock Shop will send an email to the person performing the “exit process” to confirm that the individual has been “cleared”.

**5.3.2 Contractors, Consultants, Vendors, and other Non-University personnel**

All keys must be returned to the FS Lock Shop at the completion of project. Written confirmation from the lock shop is required before final payment is made.

**5.4 Lost, Stolen, Un-returned and Broken Keys. Lost or Compromised Codes**

**5.4.1 Lost Keys/Codes**

1. Lost keys/codes are to be reported to the Department Manager and to the Police Department.
2. A new key request procedure must be initiated for replacement keys/codes. A Work Order should also be submitted with the appropriate accounting string.
3. Each department is responsible for the total cost of lock changes, reprogramming, and new keys/codes to secure areas compromised by lost keys/codes.

**5.4.2 Stolen Keys/Compromised Codes**

1. If a key/code is stolen or compromised it must be immediately reported to the Department Manager and to the Police Department.
2. A detailed police report must be filed detailing the circumstances of the theft.
3. A new key request procedure must be initiated for replacement keys/codes. A Work Order should also be submitted with the appropriate accounting string.
4. Each department is responsible for the total cost of lock changes, reprogramming, and new keys/codes to secure areas compromised by stolen keys.

**5.4.3 Un-Returned Keys**

1. It is the responsibility of the authorizing department to make every effort to secure keys from personnel terminating employment or students leaving school. If efforts fail to obtain the keys they should be considered lost.
2. Each department is responsible for the total cost of lock changes and new keys to secure areas compromised by lost keys.

**5.4.4 Broken or Damaged Keys**

1. If a key is broken or otherwise damaged the pieces must be returned to the departmental key coordinator or the FS Work Center. If a key is broken off in a lock or is malfunctioning notify FS Work Center immediately.
2. A new key will be issued after damage verification. There is no charge for the replacement.

**5.5 Building Hours**

Building hours are not typically posted on each building as they vary based on actual usage, day of the week, semester, special event, etc. As such, the department or division with primary use/control of the building will submit a schedule to the FS Lock Shop for programming.

1. Building hours are programmed in accordance with the occupant’s submitted schedule or Toggled open by occupants. Building occupants take responsibility for opening and closing their space (i.e. Student Union, Broome Library, Student Housing, Tenants.)
2. All general use classroom (excluding labs) and public use conference rooms are scheduled to be open during regular business hours.
3. Labs will be programmed on a schedule or access by code/card only.

**5.6 Inventory**

The recorded inventory of keys, codes, cards and fobs is maintained in the FS Lock Shop. Digital record keeping is maintained for Sitemaster, SMS and CPAM. Hard copy logs, where each recipient signs for the credential i.e. key, code, card, fob, are also maintained in the OPC Lock Shop.

**5.7 Extreme Security Areas or Locks Removed From the University Master Keying System**

Circumstances may occur that result in specific areas within the University requesting removal from the master keying system. Since removal eliminates the usual custodial, maintenance, and emergency services, special authorization and procedures are needed. A representative with a key would be required to unlock the space and be present while maintenance or custodial work is done.

1. These specific areas will normally fall in the High Risk or High Security categories such as the President’s Office/Suite, AIT Data Closets (See ICSUAM 8080.0, <http://www.calstate.edu/icsuam/sections/8000/8080.0.shtml> for more information.), Cashiers Office, ATM Room, Human Resources, Payroll, University Police evidence room, controlled substance storage rooms, etc.
2. Written requests for such special keying will be forwarded from the appropriate AVP, Dean or Director to the Building Access and Security Systems Control Task Force for consideration. Please note that Standard University locksets and keyways are still required for these areas.
3. With approval of the Building Access and Security Systems Control Task Force, the FS Lock Shop will key University locks off all Master's and cut individual door keys only at the direction of the requesting AVP, Dean or Director. It is understood that even though no other keys will exist for the specified areas the FS Lock Shop and University Police would still not be "locked out".
4. In the event of an emergency and the University Police are unable to contact the individuals having keys and forcible entry is necessary the department will be responsible for repairs.

**5.8 Electronic Access System**

A new electronic access system now being incorporated on campus is the Cisco Physical Access Control/Manager system (CPAM). The CPAM system is scalable and flexible, able to manage up to several thousand doors. The University can combine modules to customize solutions, and can manage the entire system remotely. The system makes use of the University issued student and staff identification card which has information coded on it. The system shall employ proximity card access readers compatible with the existing “CI One Card” cards. In some cases, a proximity reader may be installed to ensure full access to the disabled. The CPAM system is managed by Academic & Information Technology (AIT) which also provides requirements for any new construction or renovation.

Selected System: Cisco Systems International, Inc., Cisco Physical Access Control/Manager system. This system shall be the University standard for electronic access.

1. Contact: For questions regarding the network system hardware and software contact AIT. For questions regarding assigning building access and locking hardware contact the FS Lock Shop.
2. General Information: It is the intent of FS to provide card access functionality to at least one exterior ADA-accessible entry (as time and resources allow). The campus department shall fund any additional controlled entries/areas. Campus departments choosing to request and fund the installation of card access systems shall also be responsible for the cost of operations and maintenance. Maintenance and administration at the building level shall be coordinated through FS.
3. Processing Requests: Campus departments desiring electronic access systems shall process their requirements through the AIT Department. Campus departments wishing to integrate existing electronic access systems with the CPAM system shall submit their requests to AIT for review.
4. Management of Electronic Systems: The CPAM infrastructure shall be centrally administered by AIT and there shall be one common cardholder database. However, due to the fact that the size and complexity of the installation is unique, it shall be the responsibility of AIT to assign local system administrative responsibility to an individual in the FS Lock Shop with the appropriate abilities, time and training. The local system administrator shall only be able to view and modify the access rights of cardholders for the areas under that administrator’s jurisdiction.
5. Key Override: All electronic access systems installed at the University must have a “key override” capability on the University keying system to allow access to building and interior areas by University Police Department, Environmental Health and Safety, and FS maintenance personnel. The only exception is detailed in “Locks Removed from the University Master Keys System.

**5.9 Traka Key Management System**

In order to reduce the number of keys carried by individuals on campus and to improve afterhours secure access to facilities, FS installed Traka Key Management Boxes (Traka Box) in all critical buildings. The Traka Box contains building access keys that are electronically tagged for control and the recording of usage. With the many elements of operation the campus deals with on a daily basis the Traka Box helps reduce the number of keys in circulation. By assigning different access levels to departments and individuals of the faculty, maintenance, custodial and security staff, the Traka Box increases coordination, safety and efficiency efforts.

Users are approved in the same manner as key and code issuance. The Traka Box provides the following:

* Ensure only authorized users have access to specific keys
* Check when a key is taken and returned, and by whom
* Identify keys that have not been returned
* Determine frequency of use of a particular key and how long for
* Notify a manager via email an alert situation

**FS Process Guideline**, Traka Box Use and Functions, provides detailed information on the use of the system.

**5.10 Special Events**

The campus is a location for numerous special events that are held by campus groups and outside entities. The locations for the events vary from buildings to open areas i.e. Quads and sport fields, but all typically need access to buildings and bathroom facilities. To facilitate access, Event Fobs have been created that can be checked out only by CI personnel.

**FS Process Guideline**, Event Fob Use and Function.

6. REVISION CONTROL

**Document Title: Building Access Protocol**

**Author:** Scott Jacobsen

**File Reference:**

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Date | Revised By | Summary of Revisions | Section(s) Revised |
| 3/23/17 | Tim Berndtson | Changed wording from Operations, Planning & Construction (OPC) To Facilities Services (FS), and Web Work to Azzier | All |
|  |  |  |  |

Review / Approval History

|  |  |  |
| --- | --- | --- |
| Review Date | Reviewed By | Action (Reviewed, Recommended or Approved) |
| Click here to enter Review Date | Click here to enter Reviewer | Click here to enter Reviewed, Recommended or Approved |
|  |  |  |