Business & Financial Affairs	**Policy Number:** FA.40.005
Approved By: Erika D. Beck	**Effective Date:** 2/4/19
President	**Page** 1 of 4

Policy on Access Management and Facility Security

PURPOSE:
The policy on Access Management and Facility Security supports regulated access to provide security for University facilities and a controlled system for keys, codes, and cards that allow access to University facilities. The policy and associated access control and security procedures establish responsibility for access authorization; inventory of locks, keys, cards, and codes; and repair and maintenance of campus locks.

BACKGROUND:
The Access Management and Facility Security Policy establishes security and access requirements for the University facilities. The policy addresses all active locking systems currently on campus and will extend to new locking systems as appropriate. The policy and procedures establish a system that assures regulated access with regard to securing University assets, and assures a controlled system for keys, cards, and codes to provide access to University facilities.

Access to facilities is essential to the smooth operation of the University. This need, however, must be balanced by an equally critical concern for the security and integrity of the facilities and their contents. It is the policy of the University to grant access to its facilities based on a rationale of need and not solely as a matter of convenience.

POLICY:
Accountability:
Assistant Vice President for Facilities Services;
Chief of Police;
Executive Director of Human Resources.

Facilities Services and the Police Department collaborate to establish the standards for access to University facilities. The Vice President for Business and Financial Affairs approves the standards and any variation from the approved standards.

Applicability:
All persons requiring access to University facilities, including faculty, staff, students, auxiliaries, lessees, contractors, and other users. Nothing in this policy supersedes any provision of any collective bargaining agreement.

Business & Financial Affairs	**Policy Number:** FA.40.005
Approved By: Erika D. Beck	**Effective Date:** 2/4/19
President	**Page** 2 of 4

Policy on Access Management and Facility Security

Definition(s):
Locks - Any fitting that is used to provide access to, and security for, any University facility.

Keys - Physical devices used to gain access to locks and include traditional cut-metal keys, electronic fobs and/or cards used in electronic locks.

Cards - Electronic lock credential uniquely encoded to a specific individual. This includes magnetic stripe, key fob, smart card, and proximity.

Access Codes -Codes used to access locks and security systems that can be used alone or in combination with a physical device. Access codes can be numerical where the User will type their personal code on the device key-pad, or be imprinted on a University-issued card where the User will swipe the card through the device.

Security System - Any physical device or technology used to detect, to record or to report the unauthorized access or use of University facilities or to detect, to record or to report criminal activity.

Facilities - All buildings, parking lots, spaces and grounds owned or controlled by the University.

Special Events - Activities other than scheduled instruction or administrative meetings. A facility may be accessed by individuals for special events occurring after hours but only if the event has been programmed in accordance with all applicable University procedures.

Text:
BUILDING HOURS
Hours for each building are appropriately posted. Faculty, staff or students that use a building's services after hours must possess a valid University issued ID Card and keys or codes issued to the individual.

KEYS/CARDS/ACCESS CODES
Access to locked University facilities required for the performance of an individual's assigned duties will be provided through the issuance of an appropriate key, card, and/or access code required for entry into the authorized area or areas. The Building Access and Security-Systems Control Board, chaired by Chief of Police, will determine the appropriate lock for each door based on number of users, type of space/facility and value of assets within.

Approved 2/4/19

Business & Financial Affairs
Approved By: Erika D. Beck
President

Policy Number: FA.40.005
Effective Date: 2/4/19
Page 3 of 4

Policy on Access Management and Facility Security

Student codes/access devices must be approved by responsible department. All requests for access must be submitted to Facilities Services using the campus key/card/code/access request procedure. It is the Department's responsibility to notify Facilities Services when a student with access privileges no longer requires such privileges.

Provost/Vice Presidents or his/her designee are responsible for determining access needs for individual staff, faculty, students, volunteers or auxiliary members. Keys, cards, and access codes must be signed for personally by the individual to whom they are issued. Individuals separating from the University must return an issued key to Facilities Services. Facilities Services will deactivate cards and/or access codes for separating employees.

Any person who knowingly lends, makes, duplicates, possesses or uses keys, cards, or access codes to allow or gain entry to University facilities without the appropriate authorization will be subject to administrative disciplinary action by the University and may be criminally prosecuted under the laws of the State of California.

Loaning and lending of keys is prohibited. Cards and access codes are the responsibility of the individual to whom they are issued and shall not be shared. Lost/misplaced keys, cards, and compromised access codes shall be reported to the area/unit Manager and to the Police Department or Facilities Services immediately. Persons in possession of unauthorized keys may be guilty of a misdemeanor as outlined in California Penal Code 469. Possession of unauthorized keys, access codes, etc., or sharing of such with unauthorized persons may constitute employee and/or student misconduct and subject the involved person to discipline.

SECURITY SYSTEMS
All security systems shall conform to standards established by the Building Access and Security Systems Control Board, chaired by the Chief of Police.

CLEARANCE CERTIFICATES
Separating faculty or staff must return all keys/access devices before clearance certificate will be signed. Campus areas/units shall notify Facilities Services of pending separations and facilitate return of all keys/access devices to Facilities Services. Human Resources shall notify Facilities Services of pending involuntary separations to facilitate deactivation of access codes at time of separation. Divisions will be held responsible for keys/access devices not returned by faculty, staff, auxiliary staff, volunteers, and

CALIFORNIA STATE UNIVERSITY CHANNEL ISLANDS
ADMINISTRATIVE POLICY MANUAL

Business & Financial Affairs **Approved By:** Erika D. Beck President	**Policy Number:** FA.40.005 **Effective Date:** 2/4/19 **Page** 4 of 4

Policy on Access Management and Facility Security

students, along with any associated costs of re-keying, as determined by Services and the Police Department.

CHARGEBACK

If keys, access codes or locks need to be reissued or replaced following a loss or an individual's failure to return a key upon separation, the Division that originally authorized the issuance of the key or access code shall be responsible for all labor and material costs associated with the reissue or replacement of all necessary equipment. The Police Department has the sole authority for determining the seriousness of the security breach and extent of the replacement of equipment required.

Replacement of door locks, re-keying or re-issuance of electronic access codes or cards, for any reason other than class schedule changes or maintenance, will be a chargeback to the requesting area/uni.

If electronic programming has to be re-done or locks re-keyed because a requester fails to pick up his/her access code within the specified time, the requesting area/unit will be responsible for the costs of re-programming or re-keying.

Issuance of keys, electronic access codes or cards for special events will be a chargeback and will be included in the facilities rental fees.

All charges related to this Policy will be processed in conformance with the University's Policy on Chargebacks.

EXHIBIT:
Policy on Chargebacks
DBFA Administrative Directive #10-01 (Access Control, Security, and CCTV Systems)