FACILITIES MANAGEMENT
Section: 530-6
Effective: 06/28/2024
Supersedes: 12/22/2020
Next Review Date: 06/28/2027
Issuance Date: 06/28/2024
Issuing Office: Vice Chancellor – Operations Management and Capital Programs

KEY CONTROL AND ELECTRONIC ACCESS POLICY

SCOPE

This policy applies to all persons at all UC San Diego locations.

POLICY SUMMARY

This policy governs the issuance and control of Building and Space Keys, Keycards, and/or Credentials at UC San Diego to ensure the safety and security of the campus community.

DEFINITIONS

A. Authorized Persons: Authorized personnel designated by Departments who are charged with the responsibility of maintaining Key Control. In the case of Electronic Access, Authorized Persons also include the Administrative Authority.

B. Buildings: Any building owned or leased by UC San Diego whether permanently affixed or mobile.

C. Check Out: Temporary Key/Keycard issuance.

D. Credentialing: Provisioning access to the assigned department group and authorized areas by the Department Access Coordinator.

E. Department: A UC San Diego department, program, organization, or group.

F. Department Access Coordinator (DAC): The personnel designated by a Vice Chancellor, Dean, Director, Department Head, or Building Manager to be responsible for authorizing, provisioning and maintaining access control transactions for the department.

G. Designated Security Integrator: A recharge support service provided by FM or by a contracted professional group to help organizations combine all their security, access and utility systems into one intelligently designed, reliable and interconnected security system.

H. Electronic Access: A type of networked lock which is opened with a Key Fob, Keycard, Keypad, Smartphone or Biometric credential.

I. Divisional Control Point (DCP): Authorized personnel designated by a Vice Chancellor, Dean, Director, Department Head, or Building Manager to be responsible for designating the Department Access Coordinator(s).

J. Electronic Access Control Program Manager (EACP): An authorized Program Manager designated by OMCP who is charged with the responsibility of maintaining the enterprise Electronic Access Control system. This role is also responsible for ensuring the consistent application of access in new Capital Projects, renovations, alterations, coordination with Facilities Management and Department Access Coordinators.

K. Enabled: The granting of rights in a software system which allows a Key, Keycard, and/or Credential to open a lock.

L. Keys: Tangible devices used to open a Physical Lock.

M. Key Control: Provision of Code, Keys and/or Credential to authorized personnel as appropriate, updating a log of the Code, Key and/or Credential holders, secure any unissued Codes, Keys and/or Credentials provided to or by the Department, and updating Electronic Access client software updated as needed.

N. Keycard: A device which, once enabled, can open an Electronic Access lock that secures a physical space.

O. Managing: Lock maintenance and rekeying.

P. Physical Lock: Mechanical devices used to secure a Space or Building. Physical Locks as described in this policy require the use of a Key to be opened. Combination, Padlock or self- administered locking devices are not included in this definition.

Q. Security Site Assessment: Examines and analyzes the actual, perceived or anticipated risks that may impact normal operations. During an assessment, a professional who has been trained specifically to identify risks and provide recommendations based on industry best-practices will review the physical location. The assessment will:

a. Determine existing security conditions and protection needed for specific location
b. Identify risks, security-related vulnerabilities and deficiencies
c. Make recommendations for improvement

R. Space: Enclosed portions of Core Funded Buildings owned or leased by UC San Diego as well as outdoor areas which are enclosed by fences or walls. Examples of a Space include but are not limited to: an office, lab, or storage area.

S. Vestibule: An interior area such as antechamber, hall, or lobby next to the external door of a building

POLICY STATEMENT

Facilities Management (FM) is responsible for Managing applicable Physical Locks and Electronic Access to Buildings and Spaces located on UC San Diego property at designated entry doors on the perimeter of the facility with the exception of UC San Diego Health Systems and Housing Dining Hospitality. FM may set fees as appropriate for this service. Electronic Access system repairs will be performed by FM or an approved vendor. The cost of repairs will be determined as follows:

1. Electronic Access Control Hardware on Exterior Doors leading into Common Areas - FM
2. Electronic Access Control Hardware on Doors leading into Department Spaces – Recharge

Both FM and UC San Diego Police Department (UCPD) are responsible for specifying new Electronic Access whether in new construction or retrofit. All installations or changes to an Electronic Access system shall be overseen by FM and UCPD, under an approved work order or building project contract.

All new system requests will require a formal, on-site, and documented Security Site Assessment.

Campus Cards office issues credentials (OneCard) and the Department Access Coordinator is responsible for provisioning access to space.

Department and Program Authorized Persons shall distribute Keys, Keycards and/or Credentials to employees as appropriate and be the initial point of contact should a lock out occur. If an Authorized Employee or Department cannot resolve the lock out, they may contact FM Customer Relations for assistance and they will provide a response as quickly as possible. FM may set fees as appropriate for this service. Upon request the unlock service requestor must provide photographic identification (campus identification credential preferred) to confirm occupancy of space. UCPD does not provide unlocking services except in exigent circumstances or emergencies.

Reproduction of UC San Diego keys by anyone other than FM is prohibited. No Keys or Keycards may be issued or duplicated without the consent of FM. It is a misdemeanor crime to duplicate, cause to duplicate, possess or use any Key or Keycard to UC San Diego Buildings or Spaces without proper authorization. Violators may be prosecuted in accordance with California Penal Code, Section 469.

Electronic Access Control Program Manager (EACP) shall periodically audit Departments to determine whether they are complying with this policy. Annually, each Department shall conduct a “self-audit” by taking inventory of all keys, keycards, and/or credentials and comparing those findings with their records. Any discrepancies shall be reviewed and corrected, as appropriate.

Building Access Standard

1. Designated entry doors will be locked and unlocked electronically, according to a predetermined schedule and will be accessible by card reader and/or CREDENTIAL entry after hours and on weekends. In some cases, card reader and/or CREDENTIAL entry may be required at all times for access to secure spaces, such as laboratories, storage locations, and other designated locations that require higher levels of security.

2. Interior doors and/or secured vestibules will be locked and unlocked according to a schedule but may not be equipped with card readers.

3. Egress only doors will remain secured at all times. These doors may also be equipped with a door monitoring contact, local sounder or piezo device that will alarm if propped or left open.

4. Perimeter doors equipped with access control devices will be equipped with door status contacts and dog-down devices shall be removed.

5. After-hours building access is granted by presenting valid access key, keycard, and/or credentials to create an audit trail. Building entrance doors will be rekeyed off building master keys to reduce the liability of lost or stolen keys. Emergency override keys will be issued to building emergency responders only.

RESPONSIBILITIES

A. FM will create and publish appropriate guidelines for Key, Keycard, and/or Credential issuance, lock maintenance, and rekeying pursuant to this policy.

B. Key, Keycard, and/or Credential holders are responsible for proper care and storage that they have been issued. If a Key or Keycard is lost or stolen, the Key/Keycard holder must report it promptly to their Department’s Authorized Person. Failure to report a lost or stolen Key or Keycard may result in disciplinary action.

C. Departments shall establish, enforce, and maintain proper Key and Access Control in their department or area. Departments shall designate Authorized Persons and provide their names to FM. Departments shall update these names with FM as appropriate.

D. Both FM and UCPD are responsible for reviewing all requests for new systems and modifications to existing electronic security systems.

E. EACP is responsible for auditing department and program Key Control compliance.

PROCEDURES

Please see Appendices and https://police.ucsd.edu/about/security/electronic-access.html

FORMS

None

RELATED INFORMATION

None

FREQUENTLY ASKED QUESTIONS (FAQ'S)

None

REVISION HISTORY

2020-12-22	The policy was reviewed as part of the 3 year policy review cycle. Edits were made to weblinks and formatting. Policy reissued.
2024-06-28	Policy revised and reissued.

FACILITIES MANAGEMENT
Section: 530-6 Appendix A
Effective: 06/28/2024
Supersedes: New
Next Review Date: 06/28/2027
Issuance Date: 06/28/2024
Issuing Office: Vice Chancellor - Operations Management and Capital Programs

APPENDIX A – Key, Keycard, and/or Credential Processes

A. Requesting Keys (Initial Issuance)

Only those service requests submitted via the FM Customer Portal by Authorized Personnel will be accepted.

1. Requirements for ordering keying services

    a. A Key or Keycard will only be issued when necessary. When access can be gained by other means (e.g., leaving doors unlocked, attended doors) a key will not be issued.

    b. When a Department receives an allocation of space, departments should consult FM regarding keying, or re-keying of the assigned space.

    c. A *Key or Lock Request Signature Authorization (including e-signature)* form signed by the Department head must be on file in the FM Customer Relations Office before any Keys or Keycards can be issued or lock changes made. The *Key or Lock Request Signature Authorization* form is available from FM Customer Relations and should be completed when a departmental or program representative is first designated or when there is a change in the Department head.

    d. Any exception to this policy must be approved by the Vice Chancellor – Operations Management and Capital Programs (VC-OMCP). The VC-OMCP can redelegate this authority.

2. Work will only be initiated after a completed *service request (SR)* has been sent to FM, processed and a work order has been issued.

3. The person designated to pick up Keys/Keycards must be an active UC San Diego employee listed on the *service request (SR),* or an individual listed on the *Key or Lock Request Signature Authorization* form on file with FM Customer Relations.

4. Keys will not be sent through campus mail.

B. Key, Keycard, and/or Credential Checkout Process

1. Where Keys/Keycards are needed for a temporary period of time by a UC San Diego Department or an outside entity providing services to UC San Diego, Keys/Keycards may be temporarily Checked Out.

2. All Checkout requests must be made at least 72 hours prior to issuance. All requests must be submitted to FM's Customer Relations Department using the FM Customer Portal.

3. All Checkout requests require a UC San Diego Department sponsor, Department IFIS index number, work order number, job number and project name.

4. Prior to making a Checkout request, every effort must be made to obtain a Key/Keycard from the sponsoring Department's Authorized Persons. If a Key/Keycard is not available, a Checkout request may be initiated.

5. Every Key/Keycard Checked Out will be at the lowest level of a keying system possible to achieve the purpose for which the Key/Keycard is being issued.

6. Only the individual designated in the Checkout request can pick up the Key/Keycard(s). Valid picture ID is required when picking up Checked Out Key/Keycard(s).

7. The loaning or transferring of a Checked Out Key/Keycard is strictly prohibited. If a Key/Keycard is loaned or transferred to someone other than the person to whom it is issued, the Key/Keycard will be confiscated, and disciplinary action may be initiated.

8. All keys/keycards shall be returned on or before the date specified on the checkout request form. If a project exceeds the return date, the sponsoring department must request an extension seven (7) days prior to the expiration date. This extension will be processed electronically using a digital or hand-signed version of the original form, with a new return date specified.

9. Key/Keycards will not be held over from one project to another (there are no exceptions).

C. Keying Services

1. The FM Lock Shop will perform the work and deliver completed Key/Keycard to FM Customer Relations. FM Customer Relations will notify customers that the Key/Keycard(s) are available for pick up.

2. Key/Keycards must be picked up at the Campus Services Complex inside Building C's north entrance weekdays between 9:00 a.m. and 12:00 p.m. Only the person listed on the service request (SR) form is authorized to pick up keys. Any person picking up Key/Keycard(s) from FM Customer Relations must provide current campus identification and sign a receipt before Key/Keycard(s) will be released. Receipt signature must match that on file with FM Customer Relations.

3. In instances where work is required to be completed onsite, FM Lock Shop employees will perform the work and leave the necessary Key/Keycard(s) with the Authorized Person. The Authorized Person will provide current campus identification and sign a receipt before Key/Keycard(s) will be released by the FM Lock Shop employee.

D. Departmental Key Issue and Control

1. Every UC San Diego Department that issues campus Key/Keycard(s) will designate a(n) Authorized Person(s) who will be responsible for Key Control for that Department's assigned Spaces and/or Building(s).

2. All Authorized Persons shall keep a written record of their Departmental Key/Keycard assignments and require a receipt signature from the individual assigned the Key/Keycard. The Authorized Person will maintain documentation showing appropriate Key Control, as detailed above, to be made available for internal audit.

3. All Key/Keycards shall remain in the sole possession of the employee to whom the Key/Keycard(s) are assigned. Loaning, borrowing, or sharing Key/Keycards is strictly prohibited. If an employee loans or shares an assigned Key/Keycard with anyone who is not authorized, the Key/Keycard will be confiscated. Key/Keycards no longer needed by the assigned employee shall be returned to the Department's Authorized Person for re-assignment or returned to FM Customer Relations.

4. Employees are required to return Key/Keycards to the Department Authorized Person upon

termination of their employment with the University. Possessing or using any Key/Keycard without proper authorization is a misdemeanor crime under California Penal Code, Section 469.

5. Department Heads are, by default, Administrative Authorities; they determine who the Department Access Coordinator will be - in most instances, it will be the current Department Key Manager.

E. Lost, Stolen, or Unreturned Keys

1. Lost or stolen Key/Keycards should be immediately reported to the Key/Keycard holder's supervisor.

2. Once they receive a report of a lost or stolen Key/Keycard, supervisors must immediately notify their Departmental Authorized Person.

3. Upon receiving a report of a lost or stolen Key/Keycard, an Authorized Person must immediately notify FM Customer Relations at (858) 534-2930.

4. If a Department is unable to return assigned Key/Keycards as required, the Department may be held fiscally responsible for rekeying costs.

F. Billing

Key or lock work requests will be billed on a recharge basis to the department requesting the work based on the information provided on the service request (SR) submitted via the FM Customer Portal.

For additional procedural information go to Blink: How to Request Key or Lock Changes.

FACILITIES MANAGEMENT
Section: 530-6 Appendix B
Effective: 06/28/2024
Supersedes: New
Next Review Date: 06/28/2027
Issuance Date: 06/28/2024
Issuing Office: Vice Chancellor - Operations Management and Capital Programs

APPENDIX B – Electronic Access Processes

A. Electronic Access Control Systems (EACS) Requests

1. Departments are responsible for all costs related to interior door access component installation, repair, and replacement in those areas including but not limited to:

    a. Keyless access that has been specified by Department stakeholders during the Capital Planning stage and installed as part of new construction projects.

    b. Keyless access that has been installed after the original building construction.

    c. Replacing standalone keyless entry systems that are not already integrated or capable of integrating with the existing enterprise-wide access control system

    d. State, federal, or university policies and/or regulations require keyless or enhanced access control to a building or area

B. Technology Standard

1. All Electronic Access systems must meet the campus standard as specified within the current design guidelines and specifications, unless exempted in writing by the VC-OMCP or their designee. All Electronic Access installations for interior doors that are initiated after the implementation of this policy shall also meet this campus standard.

2. All Electronic Access hardware that does not interface with or meet the campus standard shall be identified and a feasibility study conducted to evaluate the efficacy of changing the system to one that meets the campus standard. All costs associated with the feasibility study and for any required conversion will be at the expense of the Department.

3. Building additions or modifications that include Electronic Access Control System (EACS) shall be communicated promptly to the Electronic Access Control Program (EACP) Manager. The Manager shall update the Department Access Coordinators (DAC) impacted and update the EACS as necessary. DACs shall notify personnel impacted by any additions or modifications to their areas. Any system updates required to provision access to the new or modified areas shall be completed by the DACs.

C. Electronic Access Responsibilities

1. Administrative Authority (AA) Responsibilities

    a. In conjunction with the facility supervisors, are responsible to designate two individuals within a facility or department area to act as primary and secondary Department Access Coordinators (DAC). Departments may assign additional DACs, depending on their specific requirements.

b. The Administrative Authority may serve as the primary DAC, or delegate other individuals in the building to serve as primary or secondary DACs. The DAC will work with the Designated Security Integrator in maintaining the department's access control and physical security systems program. Failure to designate a back-up DAC could delay processing of access transactions when the primary DAC is unavailable.

c. The name and contact information of the assigned Administrative Authority and their backup and any changes in this capacity must be sent to FM and EACP Manager.

d. Departments are responsible for controlling and scheduling electronic card reader and/or CREDENTIAL access to building entry and perimeter doors and to all areas assigned to, or under, the department's control and responsibility.

e. The department authorizing access for an individual is responsible for removing, returning, or revoking the access as required. This includes any metal keys or electronic access devices issued to allow access to department-controlled areas.

2. Department Access Coordinator (DAC) Responsibilities

a. Obtain authorization from their Divisional Control Point (DCP) or Director to requisition new EACS or initiate modification of existing EACS. All installations and modifications shall comply with university policy and standards and be conducted by or under the oversight of Planning, Capital Program Management or FM.

b. Implement department access control procedures.

c. Managing electronic card reader and/or credential access to building entry and perimeter doors and other card access areas under the department's control

d. Granting or removing card reader authorization for user access to building entrances and other areas under the department's control, including granting and removing access for new employees, departmentally sponsored visitors, retiring employees, terminated employees, and rotating student access as required.

e. Provisioning door schedules for the facility or area under their control.

f. Routinely contacting the Designated Security Integrator to re-authorize individual card-reader access users, based on the level of access and security required (The DAC should authorize the minimal level of access required for an individual to perform their assigned duties or responsibilities).

g. Terminating any means of electronic access to building perimeters or other university areas under their control when the user or employee leaves the department or university.

h. Maintaining accurate records for individuals who have been granted electronic access to building perimeter doors and all other areas under the department's control.

i. Routinely evaluate access control systems and requested modifications for functionality and effectiveness.

j. When EACS or access permissions to buildings or rooms change (departmental space changes, doors are added, rekeyed, or reprogrammed), the DAC shall notify FM and UCPD so that affected users (ITS, Campus Fire Marshal etc.) are notified appropriately.

3. Divisional Control Point (DCP) responsibilities:

a. Document DACs, telephone number, email, department name and building location; and shall send the information to the relevant DCP for compiling into a master list of DACs for the relevant division.

b. Each DCP shall send their divisional master list of DACs to the EACP designees in FM and

UCPD.

c. Departments are responsible for notifying DCPs of all changes to their department delegations.

d. Create and maintain their divisional master lists of DACs up to date and for promptly sending updated lists to the EACS designees in FM and UCPD.

e. Only DACs on the master list are authorized to request EACS actions.

4. Facilities Management (FM) responsibilities:

   a. Performing or managing all lock work, EACS readers and door hardware repair for campus managed facilities.

   b. Review and fulfill Work Order requests for EACS issues and recovering costs as applicable.

   c. Assisting in the on-boarding of new EACS systems and devices during the commissioning of a Capital Project or Renovation at a recharge.

   d. Assisting in the training of new DACs to include one-on-one, group, and facility commissioning of Capital Projects or Renovations at a recharge.

   e. Ensuring scheduled closures such as holidays are, by default, programmed to automatically secure facilities.

5. EACP Manager responsibilities:

   a. Ensure that the electronic access control system server is online and functioning.

   b. Validate the redundant, failover system server is functioning and tested quarterly.

   c. Request and ensure proper backup and system firewall templates are applied and maintained.

   d. Maintain system records, including purging transactions every 12 months to maintain system performance.

   e. Coordinate system-related activities between the Integrator, ITS, and DACs as appropriate to ensure successful device installation.

   f. Troubleshoot and resolve system-related problems.

   g. Actively audit system account management.

   h. Document and submit change management requests for proper approval as required for any change that may affect system-wide end users and departments.

   i. Schedule and perform system-level housekeeping and audit activities to ensure optimal system operation.

   j. Coordinate formal training programs and documentation to on-board new DACs and FM personnel.