UC SANTA BARBARA POLICY AND PROCEDURE

Physical Access Control
Contact: Administrative Services
Issued: June 24, 2013
Supersedes: Keys - Administration and Control of Keys, September 2007; and
Keys - Issuance and Retrieval, March 1986
Pages: 13

PHYSICAL ACCESS CONTROL

OVERVIEW

The purposes for physical access controls are to enhance the personal safety of the campus community and to secure University property. A successful program is dependent on every member of the community being diligent in the stewardship of physical access devices and alert to their surroundings. The implementation of physical access controls must be balanced with the University's value of being an open and welcoming place to study, teach, research, and collaborate.

I. SCOPE

The policy applies to all members of the campus community and governs physical access controls for all facilities managed by UCSB (University facilities). Physical access controls may involve mechanical key systems, specialized security access systems, lockbox systems, card access control systems, or any system designed to control room or facility egress.

II. DEFINITIONS

See Appendix A.

III. POLICY

A. Physical Access Controls

1. To enhance the safety of the campus community and its assets and assure compliance with applicable building safety, fire and life safety codes, and the Americans with Disability Act (ADA), only University authorized access controls shall be used on University facilities.

2. All access control systems installed in University facilities shall comply with campus standards, unless exempted in writing by the senior associate vice chancellor for Administrative Services.

3. All installations or changes to access control systems and equipment shall be performed by or overseen by Campus Design and Facilities, under an approved work order or building project contract.

4. Unauthorized locks or suspicious looking access controls (such as chains looped through door handles) must be reported to the Police Department, as soon as possible. The Police will contact the department access controller (DAC) or business officer to determine whether the locks are unauthorized. In an emergency situation or if the unauthorized locks create a safety violation, the Police shall remove the lock(s) or shall contact Campus Design and Facilities Customer Service to remove the lock(s). In ordinary situations, when the DAC becomes aware of an unauthorized lock, s/he shall have it removed by the department or shall send a work order request to Campus Design and Facilities Customer Service to have it removed, to ensure the safety of the campus community and compliance with this policy.

B. Physical Access Control Devices

1. All department and unit heads must establish and maintain controls for the issuance, possession, and storage of all access control devices that provide access to University facilities and vehicles. Access control devices may include but are not limited to mechanical keys, key cards, fobs (for limited short-term use), and keypad data.

2. Access control cards for University facilities shall be obtained through the University Center Access Card unit, with one exception. The Police Department may produce access control cards for Police Department employees.

3. Mechanical keys and fobs for University facilities shall be obtained through Campus Design and Facilities Customer Service.

4. Access control devices that provide access to University facilities and vehicles are the property of the University of California and must be returned when: a) requested by the issuing department, b) the business necessity for access ends, or c) in response to a lawful order.

    a. If the access control device is an access card or other electronic device, the department shall advise its DAC to deactivate the department's access authorization when access to that department's assigned space is no longer a business necessity.

    b. When an access control device is no longer needed, it must either be securely destroyed or stored depending on the type of device. If the access control device holder is ending his/her affiliation with UCSB, and the access control device contains an individual's image, the department shall deactivate access authorizations and securely destroy the access control device. If the returned access control device is a mechanical key or generic electronic device (such as a fob, as might be issued to short term visitor scholars or contractors), the department shall deactivate access authorizations on the electronic device and securely store the mechanical key or generic device and update the department's inventory log. The DAC shall notify (email) the campus access control database administrator to ensure the campus access control system database remains up-to-date.

    c. Excess access control devices (such as mechanical keys or fobs) that are no longer needed by a department shall be hand delivered to Campus Design and Facilities Customer Service. Department inventory logs shall be updated to record the transfer of the access control devices to Campus Design and Facilities Customer Service.

5. The loss or theft of a University access control device shall be reported to the DAC as soon as possible, but no later than 24 hours from the loss or theft. The DAC shall deactivate access authorizations on electronic device(s) and notify the campus access control database administrator to ensure the campus access control system database remains up-to-date. If level A1 or A2 mechanical master keys (see Appendix B) are lost or stolen, the DAC shall report the loss or theft to the UCSB Police Department.

IV. RESPONSIBILITIES

A. The senior associate vice chancellor, Administrative Services (or designee) serves as the campus access control director and is responsible for the campus access control program. S/he shall review all requests for new access control systems or modifications to existing access control systems that diverge from campus standards. The review shall be in consultation with the relevant executive vice chancellor or vice chancellors, and chief of Police (or designee). Exceptions to the campus standards or this policy require approval from the campus access control director.

B. Campus access control device providers are the University Center (access cards) and Campus Design and Facilities (mechanical keys and short-term-use fobs). These specified access control device providers are the only departments authorized to fabricate or requisition and distribute access control devices for UCSB managed facilities and vehicles, with two exceptions: 1) when original keys are furnished directly by the manufacturer, under new (building or alterations) contracts and 2) the Police Department may fabricate or requisition electronic access card devices for the Police Department. Campus access control device providers are responsible for implementing procedures for fabrication, issuance, inventorying, tracking, and securing devices under their control and for documenting access control transactions.

C. Campus access control managers (CACMs) are responsible for the administration of access control systems and procedures within their designated areas, in coordination with the campus access control database administrator. CACMs are:

Housing and Residential Services - for all residential housing;
Police Department - for Police Department employees;
University Center - for the UCen and Thunderdome; and
Campus Design and Facilities (Customer Service) - for all other University facilities.

CACMs, for their designated areas, shall:

1. Implement access control procedures and secure access control system(s). Security measures are to meet or exceed standards presented in UC Business and Finance IS-3, Electronic Information Security. These include partitioning access control privileges internal to UCSB; protecting against external unauthorized access; and having backup and recovery systems and procedures.

2. Provide training to new department access controllers in their designated area(s).

3. Maintain accurate records of all access control transactions. Transaction records shall be moved into the access control system's archive at the end of each fiscal year. Transaction records shall be retained in the archive for five fiscal years after their deposit and thereafter destroyed. All stored access control records are subject to audit.

4. Ensure relevant emergency access control devices are secured in lock-boxes and kept up-to-date to assure timely entry into all buildings by authorized emergency personnel.

5. Add, extend, or deactivate authorized access control devices as authorized by the campus access control director or department access controllers, and consistent with this policy. (DACs may activate or change department level authorized access permissions for active access control devices. See Section III.F.)

6. Maintain an inventory of and secure unissued access control devices.

7. Document and maintain records of the destruction/recycling of any defective devices.

8. Consult with Chief of Police (or designee) and DAC regarding lost or stolen mechanical master access control devices (level AL1 or AL2, Appendix B) and affiliated risks or concerns.

9. Routinely evaluate access control systems and requested modifications for functionality and effectiveness. Re-key mechanical systems as appropriate. All installations and modifications repairs and maintenance shall comply with University policy and standards and be conducted

by or under the oversight of Campus Design and Facilities, unless otherwise authorized in writing by the senior associate vice chancellor, Administrative Services (or designee). Requests for repair or re-keying shall be administered according to campus policies and Campus Design and Facilities procedures.

D. Campus Design and Facilities Lock Shop is solely responsible for**:**

1. Performing all lock work for campus managed facilities, except work performed by contractors working under the direction of Campus Design and Facilities.

2. Fabricating and duplicating (or overseeing the fabrication and duplication of) mechanical keys for all campus managed facilities.

3. Issuing mechanical keys to authorized DACs for re-issue within their department; obtaining DAC signatures on key issuance; and maintaining and securing records of key transactions in accordance with UC Records Retention Schedules and University policy.

4. Recovering costs for mechanical keys and lock work in accordance with an authorized work order.

5. Inventorying and securely maintaining unissued mechanical key stock.

E. Each divisional control point is responsible for ensuring their deans, directors, department chairs, and administrative officers designate department access controllers and oversee the implementation of this policy for their respective areas.

1. Departments shall document: the access controller's name (and alternate's name, as appropriate), telephone number, department name and building location; and shall send the information to the relevant divisional control point for compiling into a master list of department access controllers for the relevant division.

2. Each control point shall send their divisional master list of department access controllers to the campus access control database administrator.

3. Departments are responsible for notifying their control points of all changes to their department designations.

4. Control points are responsible for keeping their divisional master lists of department access controllers up-to-date and for promptly sending updated lists to the campus access control database administrator in Campus Design and Facilities Customer Service.

5. Only the designated access controllers on the master list and the campus access control director (or designee) are authorized to request access control actions from the campus access control database administrator.

F. Department access controllers (DACs) are responsible for the access control procedures for their designated areas. DACs shall:

1. Obtain authorization from their dean/director/chair to requisition new access control systems or initiate the modification of existing access control systems and send the authorization to Campus Design and Facilities. All installations and modifications shall comply with university policy and standards and be conducted by or under the oversight of Campus Design and Facilities.

Deviations from campus standards require the prior written approval of the senior associate vice chancellor, Administrative Services.

2. Implement department access control procedures.

3. Review requests for access and, when determined appropriate for University business purposes, initiate the process for obtaining an access control device from the relevant access control device provider (Section IV.B.). The campus standard is to issue one access control device per individual, per access control system. Individuals who have already been assigned more than one device per access control system may retain the 2nd device until they separate from the department, but are requested to return any additional devices to their DACs.

4. Once the access control device has been created:

   a. For mechanical keys:
      1) The DAC shall pick up the keys from Campus Design and Facilities. The DAC (or designee) will present identification at pickup and sign for the keys. Keys shall not be sent through the mail. If lock work is completed on-site, keys will be given only to the DAC (or designee), subsequent to obtaining the DAC's (or designee's) signature on the receipt.

      2) The DAC shall issue the key(s) to the department authorized recipient; obtain a signature from the recipient; and retain a record of the issuance and receipt.

   b. For electronic access control devices:
      1) The device holder will bring the device to the authorized DAC.

      2) The DAC shall activate access permissions that have been authorized by the department that manages the space, using the campus access control system software.

      3) The DAC shall retain a record of the authorizations.

   c. For every device issued, the DAC shall notify the device holder of his/her stewardship responsibilities (see Section IV.G-H.); and shall retain records that document the device number, name of recipient, date of issue, access permissions given, date of return or loss, and date permissions were deactivated. Records shall be retained in compliance with the UC Records Retention Schedule and secured and disclosed in compliance with University policy. All department access control records are subject to audit.

   d. Maintain an inventory of and store unassigned department access control devices in a secure location with restricted access. Document and retain records of the destruction of any defective devices.

   e. Recover or disable access control devices, upon employee separation from the department, the end of the contract term, or completion of the business necessity for access. Departments should consult with Human Resources – Labor Relations or Academic Personnel if they intend to have their DAC recover or deactivate an access control device assigned to an employee on a long term leave, investigatory leave, or when absence from the campus is for an extended period of time. If the individual is separating from the University, within a week of separation, notify the campus access control database administrator to deactivate the access card.

f. Verify annually, in consultation with the department business officer, that employees (who have been issued access control devices) are employed by the department and that their access privileges are up-to-date. Routinely verify that access privileges for contractors**,** guests, vendors, or volunteers are still justified for University business purposes. If access is no longer appropriate for the access control device holder, recover the access control device(s) and if an electronic device revoke their access authorization. If the individual has separated from the University, within a week of separation, notify the campus access control database administrator to deactivate the electronic access control device(s).

g. Report unrecovered, lost or stolen mechanical master access control devices (level AL1 and AL2 - Appendix B) to the Police Department. Report all missing access control devices to the department business officer for a risk evaluation.

5. Departments are responsible for all costs associated with mechanical key replacement and required re-keying of locks due to the loss of an access control device by their access control device holder. If the same access control device holder subsequently loses another access control device, a department may consult with Human Resources to determine whether they can recover the costs from the access control device holder directly. If repeated losses occur, departments may consider revoking the access control holder's privilege of being assigned an access control device.

6. When access control systems or access permissions to buildings or rooms change, e.g. doors are added, rekeyed, or systems are reprogrammed, the DAC shall notify the Police Department, Communications Services, Information Technology (in OIST), Campus Fire Marshal and other affected users and activate new access authorizations, as appropriate.

G. All individuals issued a university access control device are required to:

1. Secure and be responsible for the access control device issued to him/her. Access control devices shall be used only by the individual to whom the access control device was assigned.

2. Return excess access control devices to their DAC. (The campus standard is one access control device per individual, per access control system. Individuals who have been assigned more than one device per access control system may retain the 2nd device until they separate from the department, but are requested to return any additional devices to their DACs.

3. Return the access control device to the department access controller upon separating from the department, at the end of his/her contract, the completion of the business necessity for access, or when requested by the DAC or supervisor. (NOTE: individuals may be liable for theft, per § 484 of the California Penal Code, if devices are not returned.)

4. Report the loss or theft of all access control devices to the department access controller within 24 hours of the discovery of the theft or loss. Individuals with access control cards enabled with other functions will also need to notify each service provider to deactivate the card for each function, such as Dining Services for meal function, University Library for book check-out, et al.

5. In addition, report the loss or theft of master mechanical access control devices to the University Police Department within 24 hours of the discovery of the theft or loss. (See Appendix B. for a description of AL1 and AL2 devices.)

H. All members of the campus community and visitors are responsible for helping to enhance the personal safety of the campus community and to secure University property by:

1. Keeping their access control devices in a safe place.

2. Not lending their access control devices to others.

3. Not propping doors open or leaving them unlocked during hours when the facility is normally closed to the public.

4. Reporting unusual access control locks or other access activity that is out of the ordinary to the DAC or Police Department.

V. TECHNOLOGY STANDARD

A. The campus standard for all electronic access control systems installed in University owned or managed facilities is Lenel On Guard. All exterior door access control systems installed in University owned or managed facilities shall meet or interface with the campus standard, unless exempted in writing by the senior associate vice chancellor, Administrative Services (or designee). Electronic access control systems for interior doors that are initiated after the implementation of this policy shall also meet or interface with the campus standard.

B. All exterior door access control systems that do 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.

C. UCSB's standard access control device is the multipurpose UCSB Access ID Card. It is an electronically programmable access card that permits access into University facilities when activated by an authorized University department access controller and campus access control database administrator. In addition, it has the capability to be used as an identification card, debit card, record work time in KRONOS, check out University Library books, and purchase meals on campus.

VI. SANCTIONS

A. Violations of this policy shall be reviewed consistent with campus practice and, where applicable, due process procedures for academic and staff employees, contract employees, students, and non-affiliates. Those found in violation of this policy may be subject to sanctions that may include: loss of access privileges; payment of replacement or rekeying costs and, in some cases, disciplinary action, up to and including termination. Departments shall consult with Academic Personnel (academic employees), Employee & Labor Relations (staff and contract employees), Dean of Students (students) or Administrative Services (non-affiliates) prior to implementing sanctions in accordance with this policy.

B. It is a crime (California Penal Code 469) and violation of University policy to knowingly make, duplicate, possess, or use access control devices to University facilities or vehicles without the approval of the University's authorized official. Violators may be prosecuted.

VII. IMPLEMENTING PROCEDURES

A. Eligibility

1. Eligibility for access control devices (cards, fobs, mechanical keys) is determined by business necessity. Campus access control managers and department access controllers shall determine access permissions in accordance with Appendix B. Deviations from Appendix B require the approval of the senior vice chancellor, Administrative Services.

2. Although all access control devices require care, those assigned master keys must take extra measures to secure the device when not in use. In general, when not in use, campus grand master keys must be physically secured in either an unmovable key safe or an unmarked locked storage cabinet/drawer in a locked area. In most cases, master keys shall not leave University property, unless the device is to be used at a remote University facility. In no circumstances shall master keys be left unattended or in unlocked vehicles or offices.

B. Physical Access Control Cards

1. The standard physical access control card shall bear the University seal, a unique identifier number, the assigned card holder's first and last name, a photograph of the individual, affiliation (such as academic, staff, student, guest), a return to name or address (access cards issued by the UCen Access Unit shall have UCen Access Desk named as the return to name/address), and a statement that the card is the property of the University of California and must be surrendered upon request by an authorized University official. Access control cards shall not, under any circumstances, display social security numbers or dates of birth. Generic, short-term access control devices may be issued provided the DAC uses the same rigorous issuance, tracking, and control procedures established for standard access control cards. The generic access control device shall not be issued to employees or students for long-term use, but may be used for contractors and department guests (such as short-term visiting scholars who are on campus less than one year).

2. Although not displayed on the access control card, the access control card has two expiration dates registered in the access control system:

    a. The access permission authorization expiration date that is set by the DAC and may be changed by the DAC at any time; and

    b. The over-riding card expiration date that is set by the campus access control database administrator.

        1) The card expiration date for faculty and staff is scheduled for ten years from the access control card issuance date. For students, the card expiration date is scheduled for five years and for contractors, visitors, and others, the access control card is scheduled for 6 months from its issuance date. Scheduling predetermined access control card expiration dates serves as a precautionary security measure that encourages regular evaluations of active/inactive access cards.

        2) DACs can view which cards are set to expire and when, and may extend the card expiration date by a request to the campus access control database administrator, if the access control card continues to be needed for University business purposes. (Note: DACs can modify *access permission authorizations* independently, at any time to meet University business need. See Section VII.B2.a.)

C. Requests for Access Control Devices

All requests for access into University managed property shall be directed to the relevant authorized department access controller (DAC). Access activation of issued electronic access control devices shall comply with this policy and the applicable campus access control manager's and the DAC's procedures.

D. Requests for Replacement Access Control Devices

1. In the event of loss or theft or a defective mechanical access control device, the assigned device holder shall notify the DAC. A replacement mechanical access control device may be issued in accordance with the department's procedure and this policy.

2. In the event of loss or theft or a defective electronic access control card/device, the assigned device holder shall notify the DAC and contact the relevant CACM for a replacement device.

    a. The CACM shall issue a replacement electronic access control device in accordance with the CACM's procedures and University policy. The electronic access control device holder shall take the replacement access control device to his/her DAC for authorization activation in accordance with the DAC's department's procedure.

    b. The DAC may activate approved access authorizations for the replacement device and deactivate authorizations for the lost/stolen/defective electronic access control device; annotate his/her records with the change; and notify the campus access control database administrator of the replacement transaction to ensure the campus access control database remains up-to-date.

E. Changes in Access Requirements due to Promotions, Relocations, Separations, Contract Expirations/Terminations

Departments shall implement procedures to ensure the department access controllers (DACs) are notified when the access requirements for an individual (employee, vendor, contractor, et al.) who has been issued an access control device have changed.

1. Access Control Cards

    a. If the change is an individual's transfer to another department, the department access controller shall deactivate the department's authorization for access; the new department's DAC may activate the same access control card with the new department's access permissions, as appropriate.

    b. If the change is an individual separating from or ending a visit to the University or a contractor whose contract is expiring, the DAC(s) shall deactivate the departments' access permissions and the home department DAC shall notify the campus access control database administrator to totally deactivate the access control device. Whenever possible, the home department DAC should try to recover the device from an individual who is separating from/leaving the University and destroy any access control device that displays an individual's name and image. A record of the destruction shall be retained in accordance with the UC Records Retention Schedules.

    c. DACs shall deactivate generic, short-term access control devices issued to individuals whose access permissions are no longer necessary for University business purposes or their affiliation with the University has changed. Changes shall be documented. DACs may place these generic access control devices in their department inventory provided they have procedures in place to secure and track them. If the department does not have a secure place to store unissued access control devices, the devices shall be sent to the campus access control database administrator for secure storage and reissuance.

2. Mechanical Keys

    a. Mechanical keys shall be recovered from transferring or separating employees or students or others whose contracts are expiring or whose responsibilities no longer necessitate

independent access. DACs may return recovered mechanical keys to the department's inventory and document the transfer or, if in excess of a department's needs, they shall be returned to Campus Design and Facilities. Their transfer shall be documented.

b. If mechanical keys are not recovered or combination locks are involved, the department access controller, in consultation with his/her department head, campus access control manager, and Police Department shall determine whether locks must be changed. The Police Department shall be notified of unrecovered keys.

F. Changes to Access Requirements due to Facility Additions or Modifications

Facility additions or modifications that involve access control systems shall be communicated to the access control database administrator. The access control database administrator will update the access control system and notify 1) affected DACs, who shall notify their affected access control device holders and 2) all Level One access control device holders. The relevant DAC shall update/activate access permissions in keeping with department authorizations and Appendix B.

G. Records Management

Records of requests, replacements, authorizations, and changes for control access devices shall be securely maintained by the department access controllers. All records pertaining to access control systems activity shall be securely maintained by the relevant access control managers. All records pertaining to campus access control database activity shall be securely maintained by the campus access database administrator. All records shall be maintained in a manner that protects the integrity and availability of the records for the duration of the retention period established in the UC Retention Schedule.

H. "Personal Emergency" Access to Buildings and Rooms

In case of a personal emergency, such as when an employee locks his/her home or vehicle keys in his/her office and can't otherwise retrieve them, the individual should first contact their supervisor, building manager, or department access controller to gain access. If unsuccessful, the individual may contact the UCSB Police Dispatch who will attempt to contact the department access controller. The individual's identity, university affiliation, and access authorization shall be verified prior to being granted access.

I. Restricted Access Areas

Departments with restricted areas that require additional access controls, such as clean rooms and specialized labs, shall develop written procedures for controlling access to the restricted areas, in consultation with the applicable department access controller, campus access control manager, Environmental Health and Safety, and the campus Police Department. The procedures shall include:

1. Eligibility requirements for access.
2. How to request access.
3. Who approves access.
4. Who issues the access control device.
5. Who will maintain and secure the access control records.
6. How will access control devices be recovered from individuals when the need for access changes, such as a change of responsibilities, separations, or contract terminations/expirations.
7. Other considerations, as appropriate.

J. Contractors, Guests, Vendors, Volunteers (Temporary Access Control Privileges)

Issuance and recovery of temporary access control devices shall be in accordance with this policy and the procedures established by the applicable campus access control managers and department access controllers. Access control device expirations shall correspond to the university business need for access privileges, as determined by the department access controllers.

K. Verification

Department access controllers, in consultation with their department business officer, shall annually verify that employees who have been issued access control devices are employed by the department and that their access privileges are up-to-date. They shall also routinely verify that access privileges for contractors**,** guests, vendors, or volunteers are still justified for University business purposes. If access control is no longer appropriate, the DAC shall recover the access control devices and deactivate access authorizations for the electronic access control devices and notify the campus access control database administrator to deactivate the electronic device(s).

VIII. RESOURCES

A. Access Card Application and Authorization Record for Departments

B. Environmental Health and Safety

C. Facilities Management

D. Facilities - Department-Funded Services and Alterations or Additions to Existing Facilities (5521)

E. Non-affiliates, Conduct of

F. Police Services and Responsibilities

APPENDIX A. DEFINITIONS

A. Access Control - Control of entry/exit to an area by any means (generally mechanical or electrical).

B. Campus Access Control Database Administrator – University career employee(s) designated to oversee, administer, and monitor the physical access control database and application; liaison with providing vendor. Contact Campus Design and Facilities Customer Service.

C. Access Control Device – A mechanical or electronic device, including but not limited to a key, an access card or electronic disk (fob), or combination lock that is used to control access to a university facility, property, or vehicle.

D. Campus Access Control Director – The senior associate vice chancellor for Administrative Services or designee.

E. Campus Access Control Managers (CACMs)– University career employees designated by 1) Housing and Residential Services, 2) the University Center, 3) Police Department, 4) the Recreational Center and 5) Campus Design and Facilities. They are responsible for overseeing the management of electronic access control system(s) for their respective areas, in consultation with the campus access control database administrator. See Section III. Responsibilities.

F. Department Access Controllers (DACs) - University career employees designated by the department head to perform department access controller responsibilities in accordance with this policy.

G. Campus Card Access System - A computerized card access control system which may be used to maintain and control access to university facilities, property, and vehicles.

H. Card/Key Access Control Records – Records maintained by department access controllers and campus access control managers that document access control transactions, including to whom a device(s) has been assigned, his/her access privileges, and the date the device was issued/recovered. These records shall contain the minimum amount of information about the person necessary for identification purposes. Social Security numbers and birth dates or other restricted (notice triggering) information must not be used, recorded, or stored.

I. Key - Any mechanical device used to operate a mechanically controlled mechanism for entry/exit to a controlled area.

J. Key Coding - Numerical combinations which control the variety of keys a department uses without jeopardizing security.

K. Knox Box (Lockbox) System - An access control system designed for emergency building access, used by service departments or police/fire personnel.

L. Mechanical Key Systems - Any mechanical device used to operate a mechanically controlled mechanism for entry/exit to a controlled area. These locks may be individually keyed or operate with a building master key.

M. Specialized Security Access Control Systems - Any specialized security lock or change of keying for special areas. These may include manual/mechanical or electrical push-button combination locks, with key-override, or other electronic system. The system provides entry access to various doors exterior to or within a building. They may provide automatic locking and unlocking capabilities of specific doors or groups of doors at prearranged times or as initiated in an emergency.

N. **University Facilities** – A facility, property, or vehicle that is owned or managed by the University.

APPENDIX B. Eligibility for Access Control Devices

Device Type	Access Level	Eligibility to Carry/Use	Approval(s) Required
Great Grand Master*	AL 1 Opens all groups of locks keyed under different Building (Grand) Masters and Knox Boxes.	Emergency operation center director, senior associate vice chancellor for Administrative Services, fire marshal, police chief, designated police/fire/EH&S personnel, designated Campus Design and Facilities employees, designated IT/communications employees.	Senior associate vice chancellor, Administrative Services.
Building (Grand) Master*	AL 2 Opens all locks within one building.	Designated Physical Facilities custodial employees (on a shift basis only), building managers, designated police/fire/EH&S employees.	Senior associate vice chancellor, Administrative Services. The relevant dean's approval is also required for issuance to building managers in academic buildings.
Department Master*	AL 3 Opens a given group of locks within a building.	Department heads (or their designees) and building managers, for those areas under their jurisdiction.	Department head.
Individual	AL 4 Opens one lock or two or more locks keyed alike (generally within one building).	Academic and staff employees, visiting scholars, students, or contracted workers as required for University business purposes.	Department head or designated department access controller; and for Housing residents, as designated by Housing and Residential Services.
Building Entrance	AL 5 Opens main exterior door(s).	Academic and staff employees, visiting scholars, students, or contracted workers as required for University business purposes. These should only be issued when an individual must work other than normally scheduled hours.	Department head or designated department access controller; and for Housing residents, as designated by Housing and Residential Services.
Utility	AL 6 Opens electrical rooms and utility closets.	Designated Campus Design and Facilities employees, building managers, designated police/fire/EH&S personnel, and designated Communication Services/IT employees.	Department Head or designated department access controller.

*Although all access control devices require care; those assigned masters must take extra measures to secure the device when not in use. In general, when not in use, campus grand masters must be physically secured in either an unmovable key safe or an unmarked locked storage cabinet/drawer in a locked area. In most cases, masters do not need to leave University property, unless the device is to be used at a remote University facility. In no circumstances shall masters be left unattended or in unlocked vehicles or offices.