University of California, Berkeley
Policy Issued:
Effective Date: PENDING
Supersedes: Policy of February 19, 1998
Next Review Date: FIVE YEARS AFTER EFFECTIVE DATE

Campus Access Control

Responsible Executive:	Vice Chancellor - Administration
Responsible Office:	Facilities Services (FS)
Contact:	Chelsea Groen, Facilities Services Customer Services Manager cgroen@berkeley.edu, 510-642-4203
Scope:	All UC Berkeley faculty, staff, students, affiliates, guests & visitors

Policy Statement

The maintenance of a safe and secure physical environment is essential to the University's academic, research and public service missions. Effective access control systems and procedures are a critical element of the University's efforts to meet this need. Concepts central to the implementation and utilization of campus access control systems include:

- Access control devices may be installed, utilized or maintained upon real property, buildings and facilities owned or managed by the University of California, Berkeley only as described and permitted by this policy.

- The Cal 1 Card is designated as the primary credential for use of the campus electronic access control system by UC Berkeley faculty, staff and students. The use of any alternate credential requires approval by the Chancellor and/or the Facilities Services Associate Vice Chancellor (AVC).

- UC Berkeley access control keys, credential codes and clearances may be issued, copied or modified only as permitted by this policy. All campus keys, credential codes and clearances, including any copies thereof, remain the property of the University and may be modified, revoked and/or recalled at any time.

- Every door, gate, or other opening with one or more access control devices must have the capacity to be overridden by a single metal key that will be available to emergency responders and University personnel with both the appropriate authority and lawful need.

- Every person (1) responsible for implementation, management or maintenance of UC Berkeley access control systems and records, or (2) requiring the issuance or use of lock box keys or other campuswide keys or clearances, must first successfully complete a criminal background check. Refer to the campus policy on criminal background checks for additional information.

- Access control systems, locations, services, privileges, directives, and functions shall be established and managed only as needed for authorized University purposes, in a manner consistent with the campus Principles of Community. They shall not be used to arbitrarily or unnecessarily monitor or restrict access to campus spaces or services in any way that perpetuates discriminatory behavior.

- The Chancellor and the Facilities Services AVC (as the Campus Access Control Director) or their designees retain the authority to alter the operation of the campus access control system during emergencies or in the face of other exigent circumstances, and may establish temporary procedures, rules and standards as necessary.

All authorities and capacities described in this policy are subject to the functional limitations of access control systems and any applicable law, policy, standards and security needs.

Scope of Policy

All UC Berkeley faculty, staff, students, affiliates, guests and visitors are responsible for appropriate use of access control systems and compliance with relevant aspects of this policy.

Certain campus units and personnel have been delegated authorities and responsibilities with regards to campus access control systems as described within this policy, and no other campus units or personnel are authorized to perform those functions without specific approval by the Chancellor and/or the Facilities Services AVC.

This policy supersedes any previous nonconforming agreement, practice or procedure.

Why We Have This Policy

Access control systems are intended to help protect life and property; to decrease the risk of injury, loss or destruction of value; to facilitate compliance with law, regulations and policy; and to reduce the potential for individual and University liability. The ideal access control system achieves these goals while providing an effective method of accountability, causing minimal impact to convenience, and incurring expense only as reasonably necessary.

Definitions

Access Control: The use of systems, devices and technologies for the purpose of restricting entry into buildings, portions of buildings and/or other facilities or areas to authorized persons and/or vehicles. For the purpose of this policy, "access control" generally does not pertain to cabinets, furniture or storage containers, whether fixed or freestanding, which lack reasonable capacity for occupancy by a person or that are temporary and transitory in nature.

Access Control Device: Includes any mechanical or electronic component installed or placed on a door, gate, barrier or other point of access that restricts entry into buildings, portions of buildings and/or other facilities or areas to authorized persons.

Access Controller: A full-time employee designated by a campus unit to supervise and maintain local access control systems mechanical or electronic as well as records.

Area of Responsibility: As used herein, the buildings, portions of buildings and/or other facilities or areas managed by a specific campus unit.

Campus Unit: As used herein, a UC Berkeley division, department or shared governance entity.

Clearance: An access control privilege that can be assigned to one or more credentials. A grouping of access controlled spaces, and/or time restrictions on access to said spaces

Credential: (or "badge") An object or device which contains and transmits a unique digital code allowing the bearer to operate an electronic access control system. UC Berkeley's primary issued credential is the Cal 1 Card.

Facilities Services Access Control/Lock and Key administration: personnel whose assigned duties include direct responsibility and authority for oversight and centralized management of campus access control systems and records.

Electronic Access Control System: An access control system that is designed to utilize a credential in lieu of (or in addition to) a metal key.

Metal Key: A usually small and metal object, specifically shaped to fit and operate a locking mechanism when presented or inserted.

Smart Key: A single device which operates both as a metal key and as a credential, and may contain additional electronic data about usage history (as may the corresponding “smart lock”) not to be confused with a key watcher system.

Stand-alone Access Control: Whether mechanical or electronic, a system of one or more devices used in lieu of metal keys and which are managed individually or through a local process rather than via the campuswide electronic access control system. Examples include push-button, digital keypad and credential reading doorknob devices.

Responsibilities

The Chancellor has overall responsibility and authority for the implementation, management and maintenance of access control systems and records for all real property, buildings and facilities owned or managed by the University of California, Berkeley.

The Chancellor has delegated the oversight and centralized management of this responsibility and authority to the Facilities Services AVC, who is designated as the Campus Access Control Director for the UC Berkeley campus and its various satellite properties, with the exception of specific properties for which this responsibility and authority has otherwise been designated.

The Chancellor has delegated the local implementation of this responsibility and authority to the head/chair of each campus division or department for any buildings, portions of buildings and/or other facilities or areas managed by that department or division.

The implementation, management and maintenance of access control systems for real property leased or temporarily occupied (but not owned or managed) by the University is recognized as the responsibility of the owner or manager of that property unless the University has specifically agreed to assume that responsibility or is otherwise obligated to fulfill it by law or exigency.

Facilities Services Access Control/Lock and Key Administration

The Facilities Services Access Control/Lock and Key administration has the responsibility and authority for oversight of all campus access control systems and records, and for the administration of this policy. The Access Control/Lock and Key administration may assess fees from other campus units for expenses incurred in the provision of service including one-time, ongoing and overhead costs.

Access Control/Lock and Key administration personnel coordinate with and support campus Access Controllers, the Facilities Services Lock Shop and outside service providers in the installation, management and maintenance of access control devices. The Access Control/Lock and Key administration advises Capital Strategies on the design of access control systems during the planning process for new or renovated buildings and facilities.

The Access Control/Lock and Key administration procures and serializes all campus metal key blanks prior to Lock Shop production and issuance. The Access Control/Lock and Key administration maintains secure storage of spare metal keys and access control devices as necessary to carry out its routine duties as well as in anticipation of public safety emergencies.

The Access Control/Lock and Key administration will develop and make available the forms and guidance needed for service requests and other administrative functions, as well as the current fee schedule for its various services which is defined by the campus recharge committee. The Access Control/Lock and Key administration Manager supervises this unit to ensure compliance with law and campus policy, and to continuously evaluate and update campus security standards and expectations. The Access Control/Lock and Key administration Manager serves as the de facto Access Controller for the campus lockbox system, the campus barrier pole system, and other campuswide access control systems.

Annually, the Access Control/Lock and Key administration shall provide a report to the Facilities Services AVC (as the Campus Access Control Director) summarizing the current status of campus access control systems and functions.

ACCESS CONTROLLERS

Each campus unit shall designate at least one (1) full-time employee as an Access Controller, with the responsibility to supervise and maintain access control systems and records within that campus unit’s area of responsibility and to serve as the primary administrative contact for the Access Control/Lock and Key administration. Additional Access Controllers may be designated as needed, and each campus unit should have at least one (1) alternate at all times.

Access Controllers are entrusted with the significant responsibility of establishing and maintaining appropriate access control security standards and procedures within their campus unit's area of responsibility. This includes developing and utilizing a comprehensive access control plan, keeping sufficient and secure records of issued keys and assigned clearances, securely storing any unissued or pooled keys and/or credentials, protecting confidential and personally identifiable information (PII) and taking reasonable measures to provide and promote accountability among those who have been assigned access privileges.

The primary Access Controller for each campus unit shall provide an annual report to the Access Control/Lock and Key administration including a summary of local access control system changes, an inventory of all issued and stored metal keys, and a list of all lost, stolen or revoked credentials.

FACILITIES SERVICES / LOCK SHOP

The Lock Shop is the unit within Facilities Services responsible for the engineering, installation and repair of all mechanical access control devices and the production of metal keys utilized on campus pursuant to this policy, only as approved by the Access Control/Lock and Key administration. Qualified Lock Shop personnel are also able to install, modify or repair electronic access control devices upon approval by Access Control/Lock and Key administration. The Lock Shop is responsible to maintain all associated standards and records associated with these functions.

The Lock Shop shall provide an annual report to the Access Control/Lock and Key administration describing the quantity, type and location of metal keys and mechanical or electronic access control devices installed, issued, repaired or replaced, held in inventory and destroyed.

CAL 1 CARD OFFICE

The Cal 1 Card office is responsible for the procurement, issuance and management of official identification cards for all UC Berkeley faculty, staff, students and other affiliates, including cards with an integrated capacity to serve as credentials for the campus electronic access control system. With the exception of utilization for the purpose of access control as described in this policy, all Cal 1 Card features and functions are within the purview of the Cal 1 Card office. Refer to the Cal 1 Card usage policy for additional information.

METAL KEY AND CREDENTIAL HOLDERS

All persons issued or otherwise in possession of UC Berkeley metal keys and/or credentials with active clearances are responsible for keeping and using them only as approved within the scope of their role(s) and in a manner consistent with this policy. This includes the duty to take reasonable precautions to prevent loss, theft, damage and unauthorized duplication. Specific responsibilities and privileges regarding the possession and use of campus metal keys and credentials with active clearances include:

- Do not leave them unattended in University vehicles or any other vehicles (whether locked or unlocked) or at any place open to the public;
- Do not duplicate them or make unauthorized copies;
- When borrowed or checked out from a shared pool, return them promptly and according to any rules or conditions;
- Without unnecessary delay, file an official police report with UCPD and notify the issuing Access Controller if they are lost, stolen or duplicated without authorization;
- Return them to the issuing Access Controller or the Facilities Services Access Control/Lock and Key administration upon separation from employment (except Student Cal 1 Cards).

Procedures

METAL KEYS

To request a new metal key, an authorized Access Controller may submit a Facilities Services Lock and Key request form to Access Control/Lock and Key administration via current procedures. The Access Control/Lock and Key administration will review the request for accuracy, completeness and consistency with policy & security standards. If approved, the Access Control/Lock and Key administration will forward the request to the Lock Shop (Facilities Services) for fulfillment. The Access Control/Lock and Key administration will assess a fee which includes the Lock Shop metal key production cost.

The Access Control/Lock and Key administration will notify the Access Controller when the new metal key has been delivered by the Lock Shop and is ready for pickup. The Access Controller may then issue the key, ensuring the keyholder signs the key issuance record (to be retained by the Access Controller). Approved Lock box keys are issued directly to the recipient and require a signature of receipt.

To request a replacement for a metal key that has been lost, stolen or damaged, the Access Controller must include the case number for the report filed with UCPD. Damaged keys should be collected by the Access Controller, logged, and returned to the Access Control/Lock and Key administration for destruction. When metal keys are lost or stolen, the Access Controller should assess whether or not any mechanical locks or other access control devices should be modified or replaced.

Production of a building master or submaster metal key (1) requires the prior approval of the appropriate building manager or facilities manager if that person is not also the Access Controller making the request, and (2) is subject to Access Control/Lock and Key administration review and approval based on an assessment of security vulnerabilities and standards.

MECHANICAL ACCESS CONTROL DEVICES

To request a new mechanical access control device or the modification or repair of an existing device, an authorized Access Controller may submit a service request to the Access Control/Lock and Key administration via current procedures. The Access Control/Lock and Key administration will review the request for accuracy, completeness and consistency with policy and security standards. If approved, the Access Control/Lock and Key administration will forward the request to the Lock Shop (Facilities Services) for additional review for compliance with fire safety and other applicable regulations and standards, and fulfillment.

The Access Control/Lock and Key administration will coordinate any necessary vendor cost estimates or project bids and prepare a summary of expected costs, to include any initial and ongoing fees charged by Access Control/Lock and Key administration. After receipt of chartstring or means of payment, and final approval to proceed by the requesting campus unit, the Access Control/Lock and Key administration and/or the Lock Shop will coordinate with the Access Controller or their designee to arrange for installation.

ELECTRONIC ACCESS CONTROL CLEARANCES AND SCHEDULES

To establish, assign, adjust or remove clearances or schedules in the campuswide electronic access control system, an authorized Access Controller may submit a request to the Access Control/Lock and Key administration and provide sufficient information to enable the adjustment. The Access Control/Lock and Key administration will review the information for accuracy, completeness and consistency with policy and security standards.

Every issued clearance requires an expiration date, set for the date the credential holder is expected not to need the clearance any longer, up to a default maximum of five (5) years from the date the clearance was issued. Credential holders and Access Controllers are responsible for renewing valid clearances as necessary, in additional increments of up to five (5) years.

Exceptions based on a credential holder's role or need may be approved by the Access Control/Lock and Key administration.

The Access Control/Lock and Key administration may approve and provide Access Controllers with a limited ability to manage the campuswide electronic access control system, so they may directly assign or remove clearances and within their area of responsibility. All schedules and other modifications must be made by FS Access Control/Lock and Key administration.

More than one Access Controller may authorize a clearance for the same credential, permitting simultaneous access within their own areas of responsibility, but only the Access Control/Lock and Key administration may authorize campuswide clearances (refer to "CAMPUSWIDE ACCESS CONTROL SYSTEMS," below).

Without unnecessary delay, Access Controllers shall notify the Access Control/Lock and Key administration of any known lost, stolen, unauthorized duplicate or revoked credential so that Access Control/Lock and Key administration staff may deactivate all clearances assigned to that credential. The Access Controller shall also ensure that an official police report has been filed with Access Control/Lock and Key administration if necessary.

For replacement University credentials, contact the Cal 1 Card office and refer to the relevant Cal 1 Card policy and procedures.

ELECTRONIC ACCESS CONTROL DEVICES

To request a new electronic access control device or the modification or repair of an existing device, an authorized Access Controller may submit a request to the Access Control/Lock and Key administration via current procedures. The Access Control/Lock and Key administration will review the request for accuracy, completeness and consistency with policy and security standards. As part of the approval process, the Access Control/Lock and Key administration will facilitate review by UCPD, Capital Strategies and/or any other University department or unit as needed, for compliance with fire safety and other applicable regulations and standards, and consideration of any other relevant issues or impacts.

Access Control/Lock and Key administration staff will coordinate any necessary vendor cost estimates or project bids and prepare a summary of expected costs, to include any initial and ongoing fees charged by Access Control/Lock and Key administration. After final approval to proceed by the requesting campus unit, the Access Control/Lock and Key administration and/or the Lock Shop will coordinate with the Access Controller or their designee to arrange for installation.

STAND-ALONE ACCESS CONTROL DEVICES

Stand-alone devices that operate solely by the manual entry of codes (whether by button, dial or other method) present an inherent and significant security concern and shall not be used for any University access control application. When such devices are installed, access codes are frequently shared, code entry can be observed by unauthorized persons, and the codes are not changed as often as they should be, if ever. Any exceptions must be reviewed and approved by FS Lock and Key administration.

Electronic stand-alone devices that rely upon existing or issued credentials are discouraged except for specific situations when no other access control option is feasible. Such devices must be actively managed, creating an administrative burden and systemic liabilities redundant to the campuswide electronic access control system. Access Controllers must individually program and maintain each stand-alone device. Damage to or malfunction of one component of a stand-alone device presents an increased risk of requiring replacement of the entire device, incurring unnecessary expense. All repairs including replacement of obsolete systems are the responsibility of the department or unit.

Options that should be considered instead of stand-alone access control devices include standard networked credential readers, IP-based networked credential readers, wireless networked credential readers, and mechanical lock-and-key systems.

SPECIALIZED ACCESS CONTROL SYSTEMS

Access Controllers may request the installation of specialized access control systems at locations with unique and/or elevated security requirements. This might include primary or supplementary access control accomplished with off-master mechanical lock-and-key systems, biometric systems, passcode systems, and/or other novel electronic and mechanical technologies. The Facilities Services Access Control/Lock and Key administration staff will review the situation with the requesting Access Controller and other campus units or vendors as needed to determine available options.

SMART KEYS

Smart key systems are labor intensive to maintain, as every individual stand-alone smart lock and smart key requires direct maintenance and programming for basic operation, and additional direct reprogramming of every responsive stand-alone smart lock is necessary upon the loss or theft of any smart key. Smart locks typically lack an integrated universal metal key override, so if utilized as the sole access control device for any occupiable space, a redundant system of smart keys must be maintained for emergency responders and others with access authority and need. In practice, smart-keys are often bulky (which presents various inconveniences for users), prone to damage and expensive to replace. Smart locks have demonstrated vulnerabilities to the elements and rough usage, and are similarly expensive to replace or repair.

Until such time as a smart key system can be identified that overcomes these flaws, smart keys shall not be utilized for access control in locations under the purview of this policy. However, campus units may self-administer smart key systems for cabinets, lockers, office furniture, safes or other storage containers, whether fixed or freestanding, that reasonably lack capacity for occupancy by a person or that are temporary and transitory in nature.

CAMPUS UNIT STORAGE OF KEYS AND CREDENTIALS

Access Controllers are responsible to ensure that any storage of UC Berkeley metal keys or credentials by their campus unit is done in compliance with this policy. In this context, "storage" means the unattended keeping for any length of time by a campus unit, including before or after issuance to the designated keyholder, for shared pool use by authorized persons, for temporary safekeeping, or for use as a spare by the campus unit.

Campus units may store up to three (3) metal keys of each type as spares, except building entry, or submaster keys, of which only one (1) spare of each type may be stored (if issuance is approved by the Access Control/Lock and Key administration staff as described in "METAL KEYS," above). Campus units may also store other issued keys for up to one (1) year, for temporary safekeeping, on behalf of the designated keyholder. No master key spares can be stored for any reason.

Campus keys and credentials may only be stored in a security container or safe approved by the Access Control and Lock and Key administration, equivalent to or exceeding one of the following standards:

1. A UL-listed "Residential Security Container" with a UL-listed group 2 lock;
2. A "Class B" burglary safe (minimum ¼-inch steel plate body and ½-inch steel plate door with a UL-listed group 2 lock); or
3. A UL-listed burglary safe with a rating of TL-15 or higher.

Keys and credentials held for shared pool use by authorized persons may be stored in a security container or safe as described above, or within a secure automated key control device approved by the Access Control/Lock and Key administration staff. Management of any such automated key control device is the responsibility of the local Access Controller on behalf of their division, department or shared governance entity.

Security containers, safes and automated key control devices shall only be installed in a room that is locked or attended at all times, and must be securely and permanently affixed to the premises unless having an unladen weight of 750 lbs or more. Access to a security container or safe, or administrative access to an automated key control device, should be strictly limited to the Access Controller(s) and their direct supervisor and/or another designated backup.

To request approval for a security container, safe or automated key control device, the Access Controller may complete and send an access control service request to Access Control/Lock and Key administration staff. The Access Control/Lock and Key administration staff will provide guidance and review the request for accuracy, completeness and consistency with policy and security standards. Upon approval, purchase and installation of the security container, safe or automated key control device is the responsibility of the campus unit.

Any campus unit that temporarily issues metal keys or credentials to authorized persons shall develop and enforce written rules for their possession, use and return. The Access Control/Lock and Key administration staff may impose additional specific rules or restrictions on the temporary issuance of campuswide keys or credentials at any time.

CAMPUSWIDE ACCESS CONTROL SYSTEMS

Certain campus units and employees may have responsibilities that require exclusive and/or specific access control over multiple locations within numerous campus buildings, portions of buildings and/or other facilities or areas. This might include units or employees responsible for the contents of various campus mechanical rooms, rooftops, service corridors, supply closets, and rooms or facilities housing telecommunications or electrical infrastructure. The campus maintains campus-wide access control systems for this purpose, including the campus barrier pole system and the campus lockbox system.

For installation, adjustment or removal of a campuswide access control device, an Access Controller for the campus unit with the exclusive and/or specific access control need may contact the Access Control/Lock and Key administration staff and submit a request by the same process as for any other access control device. The campus unit with the exclusive and/or specific access control need is responsible for all installation and maintenance costs of such devices.

Electronic access control devices may be utilized within campuswide access systems, but only the FS Access Control Administration is authorized to grant campuswide clearances, which may be requested by Access Controllers as described in “ELECTRONIC ACCESS CONTROL CLEARANCES,” above.

Access Controllers may request the issuance of campuswide metal keys for persons with the appropriate need and authority by sending an access control service request to the FS Access Control/Lock and Key Administration. The requesting campus unit is responsible for the cost of this key procurement and any additional fees if applicable.

Campuswide metal keys may only be carried by authorized persons when engaged in work-related activity, and may only be used for a valid work-related purpose. When not carried, campuswide metal keys shall be stored securely at a UC Berkeley worksite, inside a locked container that is not easily movable, and which is kept inside a locked room not generally accessible to the public.

To facilitate accountability, minimize the risk of loss and theft and reduce costs, campus units with two (2) or more persons requiring the use of campuswide metal keys may be required by the FS Access Control/Lock and Key Administration to securely store those keys in a central location as a shared pool, allowing authorized users to check out those keys on a daily basis as needed. Refer to “CAMPUS UNIT STORAGE OF KEYS AND CREDENTIALS,” above.

Any campuswide metal keys that are not individually assigned to a current employee or held as part of an authorized shared pool shall be delivered without unnecessary delay to the FS Access Control/Lock and Key Administration, whether by the keyholder, the keyholder’s local Access Controller or by any other supervisor or employee who receives, posesesss or discovers such keys.

Upon the report of any missing campuswide metal keys, the FS Access Control/Lock and Key Administration shall determine if any or all of the corresponding campuswide access control devices should be adjusted or replaced, in consultation with the Lock Shop and the relevant campus unit(s).

Unless otherwise agreed upon or directed by the Chancellor or the Facilities Services AVC (as the Campus Access Control Director), the cost for adjustment or replacement of campuswide access control devices necessary as the result of missing campuswide metal keys shall be divided evenly between the keyholder’s campus unit and the campus unit(s) controlling each affected location (or fully by the latter if it is not reasonably possible to identify the keyholder’s campus unit).

CAMPUS BARRIER POLE SYSTEM

The campus barrier pole system is a specific campuswide access control system managed by the FS Access Control/Lock and Key Administration intended to deter unauthorized and potentially dangerous access of vehicles to campus service roads, paths, plazas and other open areas, but also to maintain authorized access to those areas by service and emergency vehicles. Unless otherwise specified and agreed upon by Facilities Services, vehicular access control for garages, gates, loading docks and at locations off the central campus are not considered part of this system, but are instead the responsibility of the controlling campus unit, and the unit is required to ensure that all emergency response groups have the proper access at the unit's expense..

Access control devices used in the campus barrier pole system (including fixed, removable and automated poles or gate-arms and their functional equivalents) are installed and maintained at the expense of FS Access Control/Lock and Key Administration, within budgetary limits as established and approved by the Chancellor. The specific placement of and minimum specifications for barrier poles are determined by FS Access Control/Lock and Key Administration in consultation with the UCPD, Fire Marshal, and Capital Strategies and in compliance with other applicable law, policy and standards.

Campus units installing or maintaining campus barrier poles that exceed minimum specifications and/or to achieve aesthetic goals do so at their own expense and only with Facilities Services approval. Any barrier pole so installed or maintained remains subject to Facilities Services access control management.

Removable or automated campus barrier poles and gate-arms should remain in a closed and secured state except when actively being utilized for entry/exit by authorized persons, or as specifically approved by Facilities Services. It is the responsibility of the last person who operated or authorized the operation of a barrier pole or gate arm to ensure it is properly closed and secured after use without unnecessary delay.

Automated barrier poles should only be operated by one person at a time and with appropriate precautions to prevent injury or damage as necessary.

Mechanical keys and clearances for the campus barrier pole system are administered by the FS Access Control/Lock and Key Administration as described in "CAMPUSWIDE ACCESS CONTROL SYSTEMS," above.

CAMPUS LOCKBOX SYSTEM

The campus lockbox system is a specific campus-wide access control system managed by the FS Access Control/Lock and Key Administration intended to enable access to all campus-controlled buildings, portions of buildings and/or other facilities or areas by persons with responsibilities that are likely to require campuswide access in routine, urgent and emergency circumstances.

Lockboxes and the keys (and any credentials) stored within them are installed and maintained at the expense of the campus unit(s) controlling that location. Specific placement and minimum specifications for lockboxes are determined by FS Access Control/Lock and Key Administration in consultation with the Fire Marshal and Capital Strategies, and in compliance with other applicable law, policy and standards.

Lockboxes shall contain at least one (1) set of metal keys that provide entry to every point of access control in each building or facility (except any campuswide mechanical keys routinely issued to campus emergency responders), and at least one (1) additional set of metal keys that provides entry to every point of access control or a purpose-specific subset of access control points in each building or facility. Keys (and any credentials) stored inside lockboxes shall be secured by an internal locking mechanism that may also be utilized to restrict or identify use by specific persons or groups.

The FS Access Control/Lock and Key Administration should audit the campus lockbox system annually to identify any deficiencies including any missing keys (and/or credentials) from within lockboxes, and to attempt to identify the keyholder who last utilized those keys, or that keyholder’s campus unit. In consultation with the Lock Shop and the manager of the building, facility or area in question, the FS Access Control/Lock and Key Administration shall determine if any or all of the access control devices corresponding to the missing keys should be modified or replaced.

The cost for replacement of missing keys from lockbox interiors shall be borne by the campus unit of the keyholder who last utilized those keys unless otherwise agreed upon or directed by the Chancellor or the Facilities Services AVC (as the Campus Access Control Director),

Metal keys and clearances for utilizing the campus lockbox system are administered by the FS Access Control/Lock and Key Administration as described in “CAMPUS WIDE ACCESS CONTROL SYSTEMS,” above.

KNOX BOX SYSTEM

The campus Knox Box system is a specific campuswide access control system managed by the campus Fire Marshal, with oversight by the FS Access Control/Lock and Key Administration, intended to enable emergency access to campus buildings, portions of buildings and/or other facilities or areas by the Berkeley Fire Department (BFD) or other fire and hazardous materials emergency responders, and also to enable emergency or authorized administrative access by campus Fire Marshal personnel.

Knox Boxes are installed and maintained at the expense of the campus unit(s) controlling that location. The specific placement of and minimum specifications for Knox Boxes are determined by the campus Fire Marshal, in consultation with Capital Strategies and BFD, and in compliance with other applicable law, policy and standards.

Knox Boxes shall contain at least one (1) set of metal keys that provide entry to every point of access control in each building or facility (except any campuswide mechanical keys routinely issued to BFD personnel for the purpose of emergency response). Keys (and any credentials) stored inside Knox Boxes may be secured by an internal locking mechanism that may also be utilized to restrict or identify use by specific persons or groups.

The campus Fire Marshal should audit the campus Knox Box system annually to identify any deficiencies including any missing keys (and/or credentials) from within Knox Boxes, and to attempt to identify the keyholder who last utilized those keys. To mitigate the potential cost and security risk of lost or stolen Knox Box keys, the campus Fire Marshal should utilize an electronic tracking system with tracking devices attached to every set of issued access keys and every set of keys stored within Knox Boxes.

The campus Fire Marshal shall file an official police report with UCPD for any missing Knox Box access or internal keys and notify the FS Access Control/Lock and Key Administration without unnecessary delay. The FS Access Control/Lock and Key Administration, in consultation with the campus Fire Marshal, the Lock Shop and the manager of the building, facility or area in question, shall determine if any or all of the access control devices corresponding to the missing keys should be modified or replaced.

The cost for replacement of missing keys from Knox Box interiors shall be borne by the campus Fire Marshal unless otherwise agreed upon or directed by the Chancellor or their designee.

The campus Fire Marshal is responsible for authorizing and managing the issuance of keys and clearances for access to the campus Knox Box system, and any other campuswide keys or clearances deemed necessary for emergency response, for BFD and other fire and hazardous materials first responders, and to authorized campus Fire Marshal personnel.

Requests for Knox Box system or campuswide mechanical keys and clearances should be completed by the campus Fire Marshal's Access Controller and submitted to the FS Access Control/Lock and Key Administration as described in "CAMPUSWIDE ACCESS CONTROL SYSTEMS," above.

ACCESS CONTROL RECORDS

To preserve the safety, security and privacy of the University and its affiliates, information collected and maintained in the course of the administration of access control systems and procedures may be withheld from public release (pursuant to Government Codes §6254 and §6255). This includes, but is not limited to, the following:

- Mechanical lock and key configurations, designs and installation details
- Electronic access control system configurations, designs and installation details
- Clearance and credential codes
- Biometric data, passcodes, passwords and passphrases
- Encryption keys, mechanisms and procedures
- Records of issued keys, clearances or other access control privileges
- Logs, journals or other historical access control system usage information
- Personally Identifiable Information (PII) and other data protected pursuant to the current campus Data Classification Standard

This section is not intended to prohibit the use of appropriately redacted or protected access control information for approved academic or administrative purposes, nor is it intended to prohibit the release of relevant information when required for an administrative investigation or action by the University, a criminal investigation by a bonafide law enforcement agency with appropriate authority and jurisdiction, or for any other lawful and mandated purpose.

POLICY VIOLATIONS AND POTENTIAL CONSEQUENCES

Violations of this policy may be reported to Facilities Services (fs-general@berkeley.edu, 510-642-1032) or to any Access Controller.

Access control devices installed upon or within UC Berkeley property without authorization by Facilities Services are subject to removal at the expense of the campus unit controlling that location.

Upon audit or review by the FS Access Control/Lock and Key Administration, any campus unit found to be in violation of this policy shall have one (1) year to correct any and all identified deficiencies. If those deficiencies remain uncorrected after that year has passed, any fees charged by the FS Access Control/Lock and Key Administration to that campus unit shall be doubled, until such time as the deficiencies are corrected.

Violations of this policy by individuals may result in administrative consequences, and disciplinary action as determined by the Office of Student Conduct (for students), the Academic Personnel Office (for faculty) or Human Resources (for other employees/affiliates). In some cases, policy violators might also incur criminal or civil consequences.

California Penal Code §469 states:

> *Any person who knowingly makes, duplicates, causes to be duplicated, or uses, or attempts to make, duplicate, cause to be duplicated, or use, or has in his possession any key to a building or other area owned, operated, or controlled by the State of California, any state agency, board, or commission, a county, city, or any public school or community college district without authorization from the person in charge of such building or area or his designated representative and with knowledge of the lack of such authorization is guilty of a misdemeanor.*

Website Address for This Policy

https://facilities.berkeley.edu/

Related Policies

Cal 1 Card Usage policy
Policy on Criminal Background Checks
Campus Security Alarms policy
Campus Security Video policy
Campus Design Guidelines
UC Berkeley Data Classification Standard

Additional Resources

Appendix: Proposal to Add or Change Policy Summary

1. **What is the name of the policy? If this is a request to change an existing policy, also give the name and approval date of the existing policy (provide a copy or website address if possible):**
   Campus Access Control Policy
   Replacing the existing "Campus Access Control policy" dated February 18, 1998

2. **Name and office of the person submitting this form:**
   Chelsea Groen, Facilities Services

3. **This policy affects (check all that apply):**

CONTROL UNITS

X Administration

□ Equity & Inclusion

□ Executive Vice Chancellor & Provost

□ Finance

□ Research

□ Student Affairs

□ Undergraduate Education

□ University Relations

CONSTITUENCIES

X Faculty

X Staff

X Students

□ Alumni

X Affiliates

X Visitors

X Others (specify): <u>Every key/clearance holder</u>

□ Specific Entities with Affected Control Units:

4. **Name and title of the Responsible Executive sponsoring this new or changed policy:**
   Marc Fisher (Vice Chancellor, Administration)

5. **Name of the Responsible Office(s) that will ensure compliance with the policy:**
   Sally McGarrahan (Associate Vice Chancellor, Facilities Services)

6. **If this is a new policy, summarize what it is and why it is needed. If this is a change to an existing policy, explain why the change is necessary:**

7. **Estimate the impact (financial, workload, etc.) of this policy on the campus:**

8. **List the names of any individuals or offices you have already consulted about this policy:**

   - Parking & Transportation, Seamus Wilmot
   - Office of the Registrar, Adam Stone
   - Information Technology, Jenn Stringer
   - Recreational Sports, Bridgett Lossing
   - Intercollegiate Sports, Josh Hummell
   - Cal 1 Office, Jorge Martinez
   - UCPD, Yoganonda Pittman
   - P&C, Eugene Whitlock
   - VCR, Elizabeth Brashers
   - Facility Managers, Cherry Chung, Alexei Anderson, Barbara Duncan, Ruben Mejia, Scott McNally, Gerardo Campos, Anthony Vitan, Brett Bibeau , Amy Robinson

- ASUC/RSSP Executive Officials, Makoto (Mako) Ushihara, Sharay Pinero