Policy Forward

The one overriding purpose for this policy is the protection of the lives and property of the Campus community. Maintaining accurate, effective access control - with both metal keys and electronic devices - is critical to protecting the Campus. The majority of thefts occur without forced entry (most probably via key), so it is imperative that proper access control is maintained. The long-term view for the campus is to have all buildings controlled with electronic card keys. The first step in this plan is to have all exterior doors to campus buildings controlled with card keys.

This policy is in place to ensure that people requesting keys actually are authorized to get them; to ensure a process of accountability for return of keys; and to resolve problems resulting from a lack of key control. This policy follows the idea that individuals and/or Departments that create a key control problem should be held accountable. Generally, this would mean the financial responsibility to correct the problem. If the problem is created with criminal intent, a legal remedy is appropriate.

The method to obtain keys is relatively simple: The person who needs a key makes a request to the person in their Department who controls keys. When the Department Access Key Controller needs a key, they request it from the Campus Lockshop (or in the case of a cardkey, from the Alarms & Access Control Unit of the Police Department).

I. Description

Access Control on the Berkeley Campus is divided into four (4) categories: mechanical key, special security key, lockbox and card access control.

This policy does not apply to stand-alone card access control systems already in place and maintained by the individual department.

A. MECHANICAL KEY SYSTEM - Any mechanical device used to operate a mechanically controlled mechanism for entry/exit to a controlled area. These locks operate with the Building Master Key.

B. SPECIALIZED SECURITY KEY SYSTEMS - Any specialized security lock or change of keying for special areas which utilize a manual/mechanical or electrical push-button, combination lock, with key-override.

C. LOCKBOX SYSTEMS - An access control system designed for building access, used by service departments or police/fire personnel.

D. CARD ACCESS CONTROL SYSTEMS - A high capacity computerized card access control system operated by the Police Department. An electronic or electromechanical device replaces or supplements mechanical key access. Card keys (normally a credit card style) are used to unlock doors. Access to specific doors by individuals, is determined by the Department Access Key Controller.

The system provides entry access to various doors within a building. Provides automatic locking and unlocking of specific doors or groups of doors at prearranged times during the day.

II. Definitions

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

B. ACCESS KEY CONTROL DIRECTOR - The Chief of Police has been designated as the overall authority and delegated the responsibility for policy, procedures, approvals and issuance of all University access keys and is accountable for the security of all campus facilities and property.

C. DEPARTMENT ACCESS KEY CONTROLLER - A full-time staff person in a given department appointed by the Department Head to be responsible for the adherence and implementation of this policy.

D. ACCESS CONTROL KEY - Any device used to gain entry/exit to a controlled system (normally a mechanical key or a card key).

E. CAMPUS CARD ACCESS SYSTEM (CAS) - A high capacity computerized card access control system operated by the Police Department serving a number of campus departments.

F. CARD ACCESS CONTROL - Access control using electronic or electromechanical devices to replace or supplement mechanical key access (normally a credit card style device).

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

H. KEY CODING - Numerical combinations which control the variety of keys a department uses without jeopardizing security.

I. KEY CONTROL MANAGER - Individual in PP-CS who manages the keying system.

J. KEY CONTROL FILE - Records maintained by the Physical Plant -Campus Services (PP-CS) Key Control Manager, based on requirements agreed upon by the Chief of Police and the Executive Director - Business and Administrative Services.

K. LOCKBOX - An access control system designed for building access,used by service departments or police/fire personnel.

III. Responsibilities

All Deans, Directors, Department Chairs, and Administrative Officers are responsible for the full implementation of this policy within their respective areas. All records are subject to audit by the Police Department

Individual Departments are financially responsible for the consequences of violations of this policy by their employees.

A. The Chief of Police is designated as the overall Access Control Director and is responsible for the following items:

1. In consultation with PP-CS, approves all new access control systems and modifications to existing systems. The appropriate Vice Chancellor will determine fund procurement for such an approved project,
2. Approves all key fabrication requests,
3. Directs Key Control Manager to conduct a key control record audit as needed,
4. Directs designated police department employees to conduct an access control system audit as needed,
5. Directs designated police department employees to conduct surveys and audits of campus departments and units to determine the level of adherence and implementation of the access control-policy, and
6. Reports the results of key control record audits of campus departments to the Vice Chancellor of Business and Administrative Services, at regular intervals.
7. Directs designated Police Department employees to oversee the mechanical and automated access control systems.

B. The Physical Plant - Campus Services Key Control Manager is responsible for creating a mechanical keying system that ensures security and convenience to departments occupying buildings or facilities and for coordinating new systems. Their duties include:

1. Maintain the key control filing system and records regarding all key systems. These records are accessible to the Police Department's Crime Prevention Unit
2. Fabricate all keys. PP-CS receives original keys, furnished under new (building or alterations) contracts directly from the manufacturer.
3. Issues all mechanical access control keys to Department Access Key Controllers.
4. Conducts all maintenance and repair work regarding mechanical locking systems.
5. Consults with Chief of Police (or designee) concerning records of keys lost or stolen. Decisions to rekey or to duplicate keys are based on consultation between the Chief of Police, the Key Control Manager, and the respective Department Head. All rekeying will be administered through PP-CS. The cost of rekeying and key-cutting is borne by the affected Department.

PP-CS is accountable to the Chief of Police for maintenance of up-to-date and accurate key control records.

C. The Department Head shall appoint a member of his/her department to be responsible for the duties of the Access Key Controller and shall advise the Chief of Police, in writing, of the departmental member assigned the responsibilities of access key controller, and their alternate. The notification should include the members' work address, telephone number and signature (for future verifications).

D. The Department Access Key Controller is responsible for developing adherence to and implementing the following:

1. Maintain accurate records of all access control activities,
2. Order and issue all department access control keys,

3. Recover University access control keys from personnel who are terminated or transferred to another department,
4. Report any failure to recover access control keys to Chief of Police, and
5. Store unassigned departmental access control keys in a Police Department-approved cabinet.

E. All University personnel are required to do the following:

1. Sign a Key Issuance Record (KC#2), cardkey application or Police Department approved form.
2. Maintain a receipt of access control keys,
3. Maintain, secure and be responsible for any access control key(s) issued,
4. Report loss or theft of access control keys to the Department Access Key Controller, and to the University Police Department within 24 hours of discovery of theft or loss, and
5. Return to the Department Access Key Controller upon terminating from the department, all access control keys issued. (NOTE: individuals may be liable for theft, under the law per section 484 of the California Penal Code, if keys are not returned.)

Any person who knowingly makes, duplicates, possesses, or uses access control (keys) to University premises, without authorization-from the Chief of Police, is punishable under the law per section 469 of the California Penal Code, which states:

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

Anyone violating this policy is also subject to administrative disciplinary actions from the University, as administered by the individual department.

IV. Eligibility

A. MECHANICAL KEYS - Eligibility to each access level is determined by the Access Key Control Director. Eligibility is as follows:

Key Type	Access Level	Eligibility to Carry
Lock Box	Highest level of key on campus; will access all buildings	Chancellor, Vice Chancellors, designated PP-CS personnel, police/fire personnel, designated PD&C personnel

Key Type	Access Level	Eligibility to Carry
Building Master	Will operate all groups of locks under different master keys within one building	Specified PP-CS Custodial Maintenance Staff (on a shift basis only), building managers, police/fire personnel
Sub-Master	Will operate a given group of locks within a building	Department Heads and Building Management personnel for those areas under their jurisdiction, and those designated by the Department Head
Individual	Will operate locks keyed alike	Faculty, staff, or students (approval from Dean or Department Head or designee)
Building Entrance	Designed to operate main door (s)	Faculty, Staff or students (approval from Dean, Department Head or designee)
"T" Keys	Will open electrical rooms and utility closets	Designated PP-CS personnel, police/fire personnel, designated PD&C personnel

B. SPECIAL SECURITY KEYING - Eligibility for changing to a security keying system is evaluated by the Crime Prevention Unit on an individual basis. Eligibility is reviewed at time of request.

C. LOCKBOX KEY SYSTEMS - Eligibility for issuance of lockbox keys is evaluated by the Crime Prevention Unit on an individual basis. Eligibility is review at time of request.

D. CARD ACCESS CONTROL SYSTEMS - Eligibility for installation for a card access control system will be evaluated by the Crime Prevention Unit on an individual basis. Eligibility is reviewed at the time of request.

Eligibility for access to controlled areas will be determined by the Department Access Key Controller at time of issuance.

V. Installation and Issuance

A. MECHANICAL KEY SYSTEMS

1. Requests: All Requests for issuance of keys and re-keying shall be submitted by the Department Access Key Controller, on a PP-CS Service Request form with justification for the key work to be performed and signed by the Department Head or the Department Access Key Controller, to the lockshop.
2. Review: All requests must be approved by the Crime Prevention Unit. The CPU will contact the requester if there are any questions or concerns. If there is no response one month after the CPU's first attempt to contact the requesting Department Access Key Controller, the request will be canceled. Approved requests are forwarded to PP-CS's Management Customer Service Center for scheduling. The Department Access Key Controller will be provided with a written explanation for any denial,

upon request. A fee will be charged to the requesting department by PP-CS for each key made.

3. Urgent Requests: For all urgent requests, the Police Department will phone PP-CS's Customer Service Center and authorize the order, or the order will be hand delivered to the lockshop. A locksmith will be dispatched by the Customer Service Center and contact will be made within 24 hours of a call.
4. Issuing Keys: The Department Access Key Controller will complete and retain a key inventory approved by UCPD. All departmental personnel shall sign UCB Form 84 prior to issuance of the key(s).
5. Exception: The only exception to this section of procedures is for Planning, Design, & Construction (PD&C) Project Managers securing keys for contractors working in unoccupied areas. In these cases, PD&C can request and receive keys directly from the lockshop. The lockshop will still maintain records and obtain signatures for these keys.

   For keys to occupied areas, the PD&C Project Manager must contact the Department Access Key Controller (DAKC) in writing at least two working days prior to date the keys are needed. If the DAKC is not known, the PD&C Project Manager must contact the lockshop. The Crime Prevention Unit then retains the responsibility to approve the request. If the request is unanswered after five working days, the PD&C manager can secure the keys from the lockshop without CPU approval.

B. SPECIAL SECURITY KEYING

1. Requests: All requests for installation of special security locks shall be made via written service request from the Department Head (or designee) to the Crime Prevention Unit or the lockshop.
2. Review: The Crime Prevention Unit will review all requests.
   a. Requests to take specific rooms off of the building master, will only be approved if the request is accompanied by a departmental purchase order for a manual/mechanical or electrical push-button, combination lock, with OMS key override.
   (1) Users of these locks are required to maintain a current list of the names of all persons who have been given the lock combination, similar to departmental lists of personnel who have been issued keys.
3. Use: No individual locks/keys may be used for space control, nor may locks be changed without approval of the Department Head and the Chief of Police. Unauthorized locks will be removed by order of the Chief of Police at the expense of the person or affiliated group in charge of that room. Unauthorized push button combination locks will be confiscated and replaced with a standard key operated lock at the expense of the person or affiliated group in charge of that room.

C. LOCKBOX KEY SYSTEMS

1. Requests: All requests for issuance of lockbox keys shall be made in writing from the Department Head to the Crime Prevention Unit. The request shall include the reason for issuing the keys, the name, date of birth and social security number of the person

being issued the keys, the length of time the keys are needed and the rate of use anticipated.

2. Review: All requests must be approved by the Crime Prevention Unit. The approval may be dependent upon a records check of the person being issued the keys. The Chief of Police shall determine when any lockbox keys issued shall be recalled from service.
3. Issuing Lockbox Keys: The Campus Key Shop shall complete and retain the key issuance record. All department personnel shall sign the record prior to issuance of the key(s).
4. Record Keeping and Key Storage
   a. The Key Shop Management shall be responsible for developing and controlling all related records relative to the issuance of lockbox keys. Records shall include:
      (1) The identity of the person being issued the key.
      (2) The person's position, work address & phone number.
      (3) A signature of the person being issued the key.
      (4) The number of keys issued.
      (5) The written justification for the issuance of key(s).
   b. Key Shop Management shall conduct an annual audit of lockbox keys to determine the rate of loss. This audit is applicable to any department or individual receiving a lockbox key.
   c. Based on the rate of loss or such related factor, the Chief of Police (in consultation with the PP-CS Key Control Manager) shall determine at what interval the lockbox system shall be re-keyed.
   d. Key Shop Management shall be responsible for the safe storage of all lockbox keys not issued or keys retrieved. A related written record shall accompany the history of any key issued.
   e. Lockbox keys issued for use may not be stored in vehicles during non-work hours. Lockbox keys should not be issued to temporary/casual employees or sub-contractors. Exceptions may be granted only by the CPU upon a written request that includes the justification, as per paragraph 1. above.

D. CARD ACCESS CONTROL SYSTEM

1. Requests: All requests for installation of card key access systems shall be submitted by the department head or PD&C Project Managers to the UC Police Crime Prevention Unit.
2. Review: Each request for a new card access control system or modifications to existing systems will result in a security survey of the facility (or facility plans) by the Police Department. The survey will include recommendations as to type and placement of equipment and detection devices. This initial survey will be provided by the Crime Prevention Unit for a nominal fee to the requesting department.
   All requests for alarm service must be approved by the Crime Prevention Unit. The request may also be reviewed by the PP-CS, if there are special requirements.
3. Specifications: Following the security survey:
   a. The Campus Card Access Control Maintenance Contractor will be notified to contact the requesting department and provide a quote for the installation of the new system within an existing building or modification to an existing system. The Campus

Card Access Control Maintenance contractor shall supply a card access control system which meets the requirements set forth in the existing Maintenance Contract to ensure that the installed system will properly interface with the Police Department's computer. The department shall notify the Police Department in writing, that they wish to proceed with the installation. Upon receipt of the intent, the Police Department will issue an approval form to be submitted to purchasing with the purchase requisitions and final approved system quote.
The purchase requisition will not be processed, without the approval form.
OR

b. For systems being installed in new buildings, a complete set of specification will be developed either by the Campus Card Access Control Maintenance Contractor or a campus approved architectural firm, and approved by the Crime Prevention Unit. The bid specifications must include applicable sections of the Card Access Control System Specifications (provided by PD&C or the Crime Prevention Unit upon request) to ensure that the installed system will properly interface with the Police Department's CAS computer.

If the Campus Card Access Control Contractor desires to bid on any project for which they have developed specification, they shall request written permission from the Purchasing Department before accepting the contract for developing the bid specification package.

Specifications are valid for one (1) year from the date of Police Department approval.

c. All procurements will be handled by the Purchasing Department, the approved bid specification and requesting department's Purchase Requisition and the Police Department's Approval form will be submitted to the Purchasing Department. Bid specifications for users who do not use the Purchasing Department will be returned to the user for processing.

All changes or modifications to any contract must have purchasing Department and Crime Prevention Unit approval before implementation. The requesting department must obtain this approval using standard Purchasing Department change order modification procedures.

The Police Department Alarm & Access Control Unit will liaison with the requesting department and the installation contractor and shall be involved in any modifications or clarifications during system installation.

4. Installation and Testing

a. The requesting department will be charged for administrative and hardware costs incurred by the Police Department in connecting the requester's system to the central system. The Crime Prevention Unit will provide a Schedule of UCPD Fees (reference Appendix A) to the requesting department.
b. The requesting department will be responsible for ordering the necessary telephone line(s) from UC Telecommunications and for paying any ongoing telephone charges. Circuit specifications will be provided by Crime Prevention Unit or Alarm & Access Control Unit.

c. The requesting department is responsible for all installation. The installer shall provide the Police Department with a complete line ready to be plugged into the central computer.
d. If an outside contractor is installing and testing the access system, the Police Department will be responsible for project review/approval.
e. New access control system and modifications to existing systems in UC-owned facilities must be inspected by PD&C for compliance with applicable codes and University regulations prior to acceptance. The requesting department shall forward an IOC to the Crime Prevention Unit for PD&C inspection services (reference Appendix B).
f. All contractors must provide as-built system diagrams to the CPU to assist the Police Department in programming their computer.
g. All access doors controlled by the card Access Control System will be equipped with a special standardized mechanical override mechanical key.

5. Orientation of the User
   a. The Police Department shall meet with the Department Access Key Controller and/or their designees to develop the security clearances and schedule of door operation.

6. Issuing of Card Keys

   a. The Police Department will issue all card access keys to the Department Access Key Controller, unless otherwise approved by the Chief of Police.
   b. The Department Access Key Controller shall obtain a completed signed Cardkey Application Form for each access card issued. This form shall be signed by the Department Access Key Controller, (or department's Key Controller designee(s)) and routed to the Police Department.
   c. The Police Department will activate in their computer all card key applications within 5 working days. Emergency requests for immediate activation will be accommodated when phone contact is made with an authorized Department Access Key Controller. The written application must be sent within 24 hours of the phone request.
   d. Lost or Stolen card access keys, shall be reported to the Department Access Key Controller and to the University Police Department within 24 hours of discovery of the theft or loss. The Police Department shall remove all lost or stolen card access keys from an active state within 24 hours of return or lost/stolen report. Written documentation shall be forwarded to the Police Department by the issuing department for all lost or stolen keys.
   e. After the initial applications are entered in to the Police Department's computer, the Police Department will provide the Card Access System user department with a list of authorized card key holder. Additional reports will be provided semi-annually.
   f. Users will be charged annually for all database changes. See rate schedule in Appendix A.

7. MAINTENANCE, REPAIR AND REPLACEMENT

a. Maintenance Agreement: All card access users, will be required to enter into a maintenance agreement with the Police Department
b. Internal Maintenance: Users capable of providing their own internal maintenance may do so at a reduced rate upon approval by the Alarm & Access Control Unit.
c. Annual Maintenance Fee: User departments will be assessed an annual maintenance fee for their systems, based on the system design and usage requirements. The annual maintenance fee is comprised of two parts:

(1) Operational costs include staffing, software/hardware support and the Campus Card Access Control Maintenance Contract which includes:

(a) Response to card access control malfunctions.

(b) Semi-annual preventive maintenance service of each user system, including a, written report to the Alarm & Access Control Unit regarding the status of each system.

This maintenance service will NOT include costs for modifications, or for repair and parts replacement necessitated by abuse or misuse as documented by the maintenance contractor.

(c) Modifications will be billed by the Police Department directly to the user department at actual cost plus an administrative fee.

(d) Documented abuse or misuse reports will, be investigated by the Crime Prevention Unit. The Police Department will be responsible for disposition of charges, and will bill the user department for the actual cost of repairs plus an administrative fee.

(2) Central System Replacement Fee - All users will be assessed an annual fee on a proportional basis for upgrades and/or replacement of UCPD's central receiving equipment.

Both amounts will be charged on a proportional basis to the individual users. This maintenance fee will be billed annually, by the Police Department.

Each user department will receive the current Schedule of UCPD Card Access Control Fees (Appendix A) with the annual bill.
d. Requests for Service to Access Control Hardware: All requests for service, whether emergency or routine, shall be made through the Alarm & Access Control Unit during normal business hours and by the on-duty Communications Officer during non-business hours. The Communications Officer shall be responsible for:

(1) Evaluating the level of service required and contacting the PP-CS after hours number and the maintenance service contractor, if necessary, and

(2) Initiating a Computer Aided Dispatch and Alarm (CADS) printout stating the problem with the system and that the Campus Access Control Maintenance Contractor has been notified. This printout shall be forwarded to the Alarm & Access Control Unit.

8. Testing: All equipment will be tested by the Campus Access Control Maintenance Contractor on a semiannual basis. Proper use of the equipment will be reviewed with the user department at the time of each test.

9. Modification and Removal of Service
a. Approval for Modifications: Approval must be obtained from the Crime Prevention Unit prior to any modifications to an existing system. Approval is necessary to ensure continued compatibility with Police equipment.

b. Discontinuance of Service: The user may discontinue service at any time. The user shall notify the Police Department and Telecommunications (if necessary). Card Access Control Maintenance fees are not refundable.

Card Access Control System Recharge Rates

1. Service Charges:

   A. Purchase of cardkeys including initial data entry:

1040/1050	$15.00
Hughes	$5.00

   B. Data Entry: Rates are based on an average of the previous 2 years activity. For new systems the rates are equal to current year's activity. See Appendix B, for a sample of the rate schedule.

2. Annual Maintenance Charges consist of:

   A. Direct System Maintenance (Access Control Maintenance Contract): The maintenance portion is calculated using the number of doors and controllers at each site.
   B. Central System Upgrades
   C. Central System Support: Central system upgrades and support are pro-rated across all card access users. Total charges (A-C) plus 15 % overhead. *(Rate schedule and methodologies subject to change)*

The policy is applicable to current and future University sites under the operational jurisdiction of the University of California Police Department, Berkeley Campus. It applies to access control systems installed in new construction or as part of any major or minor capital improvement project.