ACCESS CONTROL

Purpose

The purpose for this procedure is the protection of the lives and property of the campus community and the District. Maintaining accurate, effective access controls is critical to protecting the campus personnel and District assets. It is the practice of the District to issue access devices that are required for the routine performance of job duties, at the lowest level that will be effective for the type of access that is needed for any given purpose.

This procedure is in place to ensure:

- requests are properly authorized;
- an individual(s) requesting an access device(s) is receiving the lowest level of device that is effective;
- a process of accountability for the return of access devices exists;
- problems resulting from a lack of access device control are resolved; and
- there is accountability when CCCCD Units have an access device control breach.

Scope

A. This procedure is applicable to all personnel employed in any capacity by the District.

B. For procedures related to technology resources refer to Business Procedure 10.54. For procedures related to asset control, refer to Business Procedure 10.55. For Employee Check-In, Employee Exit, and Asset and Access Device Assignment forms, refer to Business Procedure 10.56. These procedures are all related, and all should be reviewed when a new employee is hired by any CCCCD Unit. When changes are made to this procedure, all related procedures should be reviewed to ensure they remain consistent.

C. This procedure is applicable to the control of access to all forms of plant, property, and equipment.

D. District employees need to be aware there are penalties for unauthorized duplication of access devices. California Penal Code, Section 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 device 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.

Definitions

A. Access Control: Control of entry/exit to a controlled space by any means (mechanical or electronic), or control of the use of equipment and fleet vehicles.

B. Access Device: Any device, whether mechanical or electronic, used to gain entry/exit to a controlled space, or that is required to use other plant, property and equipment.

C. Access Device, Controlled Space: Any device, whether mechanical or electronic, used to gain entry/exit to a building, storage area, equipment yard, or other related controlled space.

D. Access Device Manager, Site: An individual in the Police Services Department who manages the physical issuance of controlled space access devices, requests mechanical devices from buildings and grounds, and whose designee records distribution and return of devices and maintains access device control records.

E. Access Device Manager, CCCCD Unit (See item G for definition of CCCCD Unit): Dean, senior dean, or department manager responsible for the area and authorized to sign access device requests on behalf of the unit.

F. Access Device Records: Records maintained by CCCCD Units and records managed by the Site Access Device Manager.

G. CCCCD Unit: An organizational element of the Contra Costa Community College District and its colleges and centers. As used in this procedure, it may be a department, division, college, campus, or center.

H. Electronic Access Device: A digital card or device used by a computerized electronic access control system for providing entry/exit to a controlled space.

I. Electronic Access System: A computerized system used to manage and operate electrically or electronically controlled devices that provide and track entry/exit from controlled spaces.

J. Mechanical Access Device: Any mechanical device (hard key or combination lock) used to operate a mechanism for entry/exit to a controlled area, or used to operate a vehicle or piece of equipment or machinery.

K. Mechanical Device System: A hierarchical set of mechanical devices used to operate a mechanism for entry/exit to a controlled area. These locks and devices form the building master device system.

L. Minor Property Recorder: A person in a CCCCD Unit that is designated to be responsible for gathering and recording the tracking and assignment data for equipment and fleet access devices held at the department or CCCCD Unit level.

M. Operating Hours: Generally 6:00 a.m. to 11:00 p.m., Monday thru Saturday at educational sites, and 8:00 a.m. to 4:30 p.m., Monday thru Friday at the District Office, on days that are not designated as District non-working days. Note: some instructional courses and special events are held during non-operational hours.

Principles

A. Access devices are District property, and may only be used in the conduct of official business, and as governed by this and other District policies and procedures.

B. Access devices will only be provided when required for the routine performance of job duties and responsibilities.

C. All managers are responsible for the full implementation of this procedure within their respective areas. All minor property records are subject to audit by higher level managers and the Director of Internal Audit Services.

D. Each employee is responsible for ensuring the security and proper recordkeeping of all assigned assets and access devices.

E. Misuse or negligent use of access devices may result in the employee being held personally responsible for replacement or costs of re-securing access to controlled access areas.

F. Assignment of access devices must be approved by a manager.

G. Outside doors are to be locked after normal operating hours. Maintenance gates and chains are to be locked immediately after passing through.

H. Unauthorized persons or suspicious activities are to be reported to the District Police Services Department immediately.

I. In order to minimize loss or misuse of assets or access devices, all asset or access device holders shall leave assets and access devices in a secure location during non-working periods. A secure location is defined as a location that is protected by at least two levels of access security, such as a locked drawer inside a locked room of a building.

J. Pursuant to District policies and procedures, employees may be subject to disciplinary action up to and including dismissal for violations of this procedure. The process and procedure for considering disciplinary action will follow the appropriate process and procedure for each employment classification per Education Code and/or applicable collective bargaining agreement.

Responsibilities

A. Access Device Holders

1. Transfer or distribution of all access devices shall be per these procedures.
2. The transfer of access devices both within and between department personnel, faculty, and students is strictly prohibited. Internal transfer of access devices between departmental personnel, and from departing employees to new employees is strictly prohibited.
3. Loss, destruction, or theft of all access devices shall be reported to department managers immediately. Loss of access devices, shall also be reported to campus police immediately.
4. Faculty, students and staff shall not unlock a building or room for another individual unless the individual is known by them to have a legitimate need to enter. These requests can be referred to the department office or the Police Services Department.
5. Authorized access device holders are not allowed to let anyone into a building or controlled space after operating hours under any circumstances except for public safety personnel if required for an emergency.
6. Tags, markings, or other forms of identification that relate a controlled space access device to a specific building or space shall not be affixed to the device.
7. All new employees shall meet with their managers to go over the District New Employee Checklist found in Business Procedure 10.56, Exhibit A, and shall sign for items received in Part B of the form.
8. When terminating employment or transferring to another work location or campus, all access devices MUST BE RETURNED during the course of completing the Employee Exit Checklist found in Business Procedure 10.56, Exhibit B. The completed checklist shall be verified and signed by the authorizing unit manager. All access devices are to be returned to the campus Police Services Department by the access device holder as a part of the exit checklist process. The departing individual should copy all records supporting the number and type of access devices returned for future reference. Individuals failing to return assigned assets and access devices prior to their departure may be held financially liable through collection, civil, or criminal proceedings for failure to return District property.
9. Adjunct faculty members who are reasonably expected to teach again at the same location/campus within a one-year timeframe do not need to complete an Employee Exit Checklist. All other departing faculty shall complete the Employee Exit Checklist and turn in all access devices prior to their last day on campus. Adjunct faculty that return to work within a one-year timeframe, that also need to be assigned an access device, shall be required to fill out only Part B of the New Employee Checklist.

B. Information Technology

1. District Information Technology department will create a Districtwide Asset and Access Device Database.
2. Provide designated unit Minor Property Recorders with access to and training on the use of the Asset and Access Device Database.

C. CCCCD Units

1. Hiring managers will ensure all new employees complete the New Employee Checklist, to ensure that employees have the proper tools, software, equipment and access devices required to perform their duties.
    a. All CCCCD units shall designate, in writing, someone to act as the unit Minor Property Recorder. A copy of the designation letter shall be forwarded to the campus or District IT manager so that the Minor Property Recorder can be authorized to access the Asset and Access Device Database to input access device holder date.

   b. The designated Minor Property Recorder will enter data for assets and access devices that are not related to controlled spaces into the Districtwide Asset and Access Device Database. Records for the issuance of controlled space access devices shall be recorded by the Police Services Department at time of issuance.
   c. Adjunct faculty that return to work following a single-year break shall only be required to fill out Part B of the New Employee Checklist, if they need to be assigned an access device.
   d. By signing the New Employee Checklist, employees accept accountability for assets and access devices assigned for their use and safekeeping. Misuse, abuse, or negligent control of assets and access devices may result in the employee being held financially and/or legally liable for the loss of use and cost of replacement of District property.

2. When equipment or fleet vehicle access devices are distributed, the Minor Property Recorder will record the access device and to whom it is assigned using the Minor Property/Equipment Checkout Log, and the CCCCD Unit Asset and Access Device Manager will have the employee sign the form indicating accountability for the devices. Misuse, abuse, or negligent control of access devices may result in the employee being held financially and/or legally liable for the loss of use and cost of replacement of District property.
3. After the Asset and Access Device Assignment Log found in Business Procedure 10.56, Exhibit C, is signed, the Minor Property Recorder will enter the access device data into the Districtwide Asset and Access Device Database.
4. When an employee separates from a department, a college, or the District, managers and supervisors shall ensure the separating employee completes the Employee Exit Checklist, prior to their last day of assignment, or the employee may be held financially and/or legally liable for the loss of use and cost of replacement of District property.
   a. At the end of each semester, unit Access Device Managers shall evaluate the status of all adjunct faculty. Adjunct faculty access device holders that are reasonably expected to teach again within a one-year timeframe shall not be directed to complete an Employee Exit Checklist. All other faculty device holders shall be directed to complete the Employee Exit Checklist and turn in all access devices prior to their last day on campus.
   b. The designated Minor Property Recorder will provide a list of assets and access devices from the Districtwide Asset and Access Device Database and attach it to the Employee Exit Checklist. The CCCCD Unit Asset and Access Device Manager shall ensure all items are returned or otherwise accounted for in accordance with this and other college and District procedures.
   c. After completion of the check-out procedure and when all assets and access devices have been returned, the Minor Property Recorder will update the Districtwide Asset and Access Device Database as appropriate.
5. It is the authorizing entity’s responsibility to make every effort to secure assets and access devices from personnel terminating employment or transferring from the department or college. If efforts fail to obtain the assets or access devices, they should be considered lost, and treated as such, according to this and other District procedures related to lost property.
6. Division and Department Managers.
   a. The CCCCD Unit Access Device Managers, in consultation with division and department managers and the Site Access Device Manager, must determine the level of access device control for their department or division that is appropriate for that organizational unit.
   b. Senior deans or college vice presidents are responsible for advising the District Police Services Department and the Buildings and Grounds managers of the

individual(s) assigned the responsibility of CCCCD Unit Access Device Manager, and their alternate(s). The notification should include the CCCCD Unit Access Device Manager and alternate's work address, telephone number and signature (for future verifications).

c. Division and department managers shall ensure compliance with related Board policies and this and other business procedures, and shall implement and maintain all required controls and records related to procurement, assignment, distribution, and collection of District access devices.

7. The CCCCD Unit Access Device Manager

a. The CCCCD Unit Access Device Manager is responsible for developing adherence to and implementing the following.

1) Report theft of devices to the District Police Services Department immediately upon the discovery of theft.

2) Ensure the unit Minor Property Recorder maintains accurate records of all equipment and fleet vehicle access devices provided.

3) Recover District devices from personnel, including students, whose employment or appointment is terminated or transferred to another department.

4) Report any failure to recover a master access device of any level to the District Police Services Department, Site Access Device Manager, and Buildings and Grounds within 24 hours of the recovery failure.

5) Retain equipment and fleet vehicle access devices in an approved, recessed (if possible), tamper-resistant lock box. (The Buildings and Grounds manager will provide specifications for approved lockboxes.)

6) Participate in access device control record audits.

D. Buildings and Grounds

1. The Building and Grounds Manager is responsible for creating and maintaining a mechanical access device (key) system that ensures security to the campus access controlled spaces, and for coordinating new systems. Following are the duties.

a. Maintain the key control filing system and records regarding all hard key systems. Ensure these records are accessible to the District Police Services Department.

b. Fabricate all original keys. Buildings and Grounds creates all newly required mechanical devices.

c. Conduct all maintenance and repair work regarding mechanical locking systems.

d. Maintain schematics, codes, product standards, and service equipment.

e. Maintain computer database of all devices, locks, and associated building and space numbers or areas that they operate.

2. Consult with the Police Services Department's Site Access Device Manager and the Director of Internal Audit Services concerning master keys that are lost or stolen. For lost master keys, decisions to re-key or to duplicate keys are based on consultation between the Police Services Department and the college President. All re-keying will be administered through Buildings and Grounds, and new access device records will be created by the CCCCD Unit Minor Property Recorders.

3. Restore physical security in a timely manner whenever key control has been compromised.

E. Police Services

1. The Director of Police, Safety, and Emergency Services (Chief of Police) has been designated as the overall authority and delegated the responsibility for building and space related access device control implementation, procedural compliance, and internal audits of device control. The Chief of Police will appoint the Site Access Device Manager.

2. The Site Access Device Manager is responsible for the following items.
   a. Ensure the Police Minor Property Recorder completes and maintains a master device inventory process.
   b. Direct Minor Property Recorder to conduct a device control record audit as needed.
   c. Direct designated Police Services Department employees to audit departmental mechanical and automated access control systems and to assist CCCCD Units with maintaining effective device control.

Access Control and Device Hierarchy Authorization

A. The hierarchy of the mechanical key systems generally utilizes the terminology below. However, when providing access to spaces using the electronic access system, the Police Services Department shall follow similar scope, area of access limitations, and approval authority as identified in this section.
   1. Great Grand Master (GGM), provides Districtwide access (electronic device only), which requires District Chancellor approval;
   2. Grand Master (GM), provides campuswide or sitewide access, which requires District Chancellor or college President approval;
   3. Master (M), provides buildingwide access, which requires approval of a vice president or senior dean.
   4. Sub-Master (SM), provides access to multiple spaces in a building, which requires approval of senior dean or dean, or as otherwise designated by the college President.
   5. Change (C) keys, devices which are the lowest level of devices in the access systems, which require Unit Access Device Manager approval.

B. No employee other than the Chancellor may authorize access device issuance for themselves.

C. Devices in these tiers will be issued strategically and at the lowest possible tier required for effective performance of duties. Acquisition of mechanical access devices is a partnership between the employee, the CCCCD Unit administrators, the Buildings and Grounds department, and the campus police.

D. Unless otherwise authorized in writing by a college President or the District Chancellor, no mechanical keys at the Master level or higher may be taken off campus.

Installation and Issuance

A. Mechanical Access Devices
   1. Requests – All requests for issuance of mechanical access devices shall be submitted to the campus Police Services Department by the CCCCD Unit Access Device Manager. The request shall be on a Key Request Form. The request form shall include justification for the work and the access device needed. This minimizes the scope for re-keying in the event the devices are lost or stolen. The CCCCD Unit Access Device Manager shall identify what building/rooms/spaces where access is required. The campus Police Services Department, in consultation with Building and Grounds if necessary, will determine the lowest level of device required to provide such access.
   2. Safekeeping – The holder of an access device to any District facility assumes responsibility for the safekeeping of the device and its use. The device will not be loaned or made available to others. When leaving a campus area(s) or building(s) or the District Office after operational hours, employees shall ensure that all doors are secured.
   3. Vendors, contractors and non-District personnel needing access to portions of District property (telephone service, elevator service, vending, etc.) are issued access devices through the campus Police Services Department. Should the device be lost or not returned upon expiration of the period of usage, vendors, contractors and non-District personnel will be responsible for all re-keying costs to all affected facilities. Prior to access devices being issued, vendors, contractors and non-District personnel are

required to sign an agreement to pay all re-keying costs for areas affected by lost or non-returned devices.

B. Electronic Access Devices

1. Requests for electronic access devices shall come from the CCCCD Unit Access Device Manager using the Device Request Form just like mechanical access devices. All electronic access devices will be issued by the campus Police Services Department. Should a CCCCD Unit wish to issue access devices to students, they must verify and attest that the student is officially and legally enrolled in the college. An end date for devices will be required for students.
2. Access Devices will be issued to those requiring entrance after regular business hours or to electronic access-controlled spaces (telecommunications rooms, computer labs, etc.) as approved by the proper CCCCD Unit authority.
3. Each person who is authorized to be in a campus building after operating hours is required to have their access device and identification with them at all times. This will enable them to enter and exit the building under non-emergency conditions. These items will also serve as authorization to be in the building should Police Services officers question your presence in the facility.
4. Certain classrooms' computer labs require the use of an access device to gain entry. If you are assigned to teach in one of these rooms, please ensure that your department has requested a modification to your access device rights so you will have access to these rooms. If you are a part-time faculty member and are teaching in one of these rooms, your department will need to process a Device Request Form to add access to each facility in which you are assigned to teach.
5. Additionally, there may be other interior rooms on campus that are departmental or sensitive in nature and are protected by the Access Device system. These include labs, server rooms, telephone switch rooms, IDF rooms, and mechanical rooms to name a few. Access to these areas is restricted and governed by the policies of the department(s) controlling those spaces.

C. Lost or Stolen Access Devices

1. Lost or stolen access devices MUST BE REPORTED IMMEDIATELY to the campus Police Services Department, the employee's manager, and the access device authorizing CCCCD Unit so officials can assess the impact of such events against building/department security. In the case of stolen access devices, the device holder shall file a theft report with the campus police.
2. Any lost or stolen device can present major security issues. The Buildings and Grounds department shall perform a threat assessment and determine which accesses, if any, should be re-keyed.
3. All costs associated with re-keying and making new devices shall be borne by the access device holder or access device holder's CCCCD Unit, not Buildings and Grounds. These costs can be substantial in the case of lost masters and sub-masters, which is why the Site Access Device Manager scrutinizes such requests to insure they are needed, proper authorizations are in place, and that the requester understands the risks involved.
4. A new access device request must be initiated for replacement devices.

D. Temporary Access Devices

1. Temporary access devices for visiting professors, temporary employees, students and contractors may be issued. The CCCCD Unit Access Device Manager shall mark the appropriate areas of the Access Device Request Form when asking for temporary access devices. Electronic access devices will also require an expiration date that will be programmed into the computerized Access Services System. Devices will not function after that date.

E. Special Security Keying

1. Any areas that are requested to be taken off the master key system so they can only be opened with a unique key or key-system are done so by exception only and must be approved by the President and the Site Access Device Manager. This approval must be in writing with the CCCCD Unit acknowledging their responsibility for the areas "off key control." Requestors should note that they are obligated to make available duplicate keys for Building and Grounds and Police Services for emergency access. Additionally, it should be noted that there will be no custodial services performed in these spaces unless prior arrangements are made with the Custodial Manager.
2. Requests – All requests for installation of special security locks shall be made via written service request from a senior dean or vice president to the Site Access Device Manager.
   a. Users/holders of these locks and access devices must be recorded in the Asset and Access Device Database.
   b. An employee or CCCCD Unit needing a special security key will complete and sign a Key Request Form for each key issued. This form shall then be signed by the Site Access Device Manager, after which it will be routed to the campus Police Services Department once the duplicate special security keys are cut, they will be issued to the employee. All records will be kept by the campus Police Services Department.

F. Master Access Devices

1. The Site Access Device Manager, in consultation with the Buildings and Grounds Manager, and the CCCCD Unit Access Device Manager will review requests for these access devices to ensure the device requested is needed and make a recommendation regarding approval.
2. Routine Audit – Master, GM and GGM device assignments will be reviewed by the Site Access Device Manager and the CCCCD Unit Access Device Managers biannually on even years. The results of the biannual audit will be forwarded to the Chief of Police and college President.

Control of Non-Building Access Devices

A. Each CCCCD Unit is responsible for equipment and fleet vehicle access devices issued within their CCCCD Unit, and an internal written inventory shall be maintained. Equipment and vehicle fleet keys shall be maintained in a locked "key cabinet" in secure location inside a lockable office inside a building. Key cabinet location and installation shall be approved by Police Services and Building and Grounds prior to the installation of the boxes. Unauthorized key cabinets, or key cabinets located in spaces other than as described in this paragraph, may be required to be moved at the CCCCD unit expense.

B. Unless authorized in writing or by position-related exception, personnel are not authorized to carry equipment keys and fleet vehicle keys when not at work.

C. For keys used by multiple parties, a traceable check-in/check-out process and log shall be established.

D. A duplicate access device for equipment and fleet vehicle shall be maintained in a separate key cabinet. The duplicate storage cabinet shall be located in a separate space from the key cabinet used for normal operations.