Title: Lock/Key/Access Control
Department: Engineering Services
Effective Date: January 30, 2019

PURPOSE

To establish procedures, roles, and responsibilities for California State University Northridge (CSUN) campus wide lock, key, and access control. An effective lock/key/access control program provides for and maintains the overall security of campus facilities and equipment through enforceable procedures for access control requirements. Access control codes and keys are State property and must not be duplicated or surrendered except as outlined herein. Keys are issued by PPM only upon written authorization of the appropriate administrative officer.

Unless otherwise described below, the Physical Plant Management (PPM) Engineering Services Lock Shop staff has responsibility for maintaining and executing tasks outlined in this Standard Operating Procedure (SOP).

This SOP applies to all organizational units of the University that utilize PPM Lock Shop services and equipment.

DEFINITIONS:

Access Codes - Codes used to open electronic locks via a physical reader. Access codes can be numerical where the user will type a code on a device key-pad or be imprinted on a University-issued card or personal driver's license where the user swipes or taps the card on a physical device. The responsible administrative officer within each department will determine the level of access to be issued to an employee. Generally, it is recommended that the responsible dean or senior administrator be assigned a building master access code; department heads be assigned an area of responsibility master access code, as appropriate; and faculty and staff be assigned an individual access code to their office and building entry door.

Administrative Officer – Those persons (e.g., academic deans, directors and department chairs and those individuals reporting to the President or Vice Presidents) authorized to approve and submit PeopleSoft requests for academic departments or administrative offices.

Authorized Key Holder – Those persons authorized by administrative officers to have in their possession and use key(s) to University facilities/equipment.

Buildings/Facilities – All buildings, parking lots, spaces and grounds owned or controlled by the University.

Executive Officers – The University President, Vice President or their delegates.

Keys – Physical devices used to gain access to rooms and areas through locks and include traditional cut-metal keys, access codes and/or cards used in electronic devices.

Key Assignments – The responsible administrative officer within each department will determine the type of key to be issued to an employee. It is recommended that the responsible dean or senior administrator be assigned a building master key; department heads be assigned an area of responsibility master key, as appropriate; and faculty and staff be assigned a key to their office and building entry door.

Lock and Key Control Program – The documentation, tracking, and accountability of building access methods and processes. This includes keys and standalone access programs; maintenance of records related to issuance, control, and return; security of structures and individual areas in connection to accessibility and the verification of authority to issue, grant and/or receive access to University buildings, facilities and any security and externally applied locking devices such as Omni and Sargent locks.

Lock Shop – Campus authority for the production of keys for all campus locks, the installation of door hardware and the programming, installation, and maintenance of Access Control Systems (Omni, Sargent, etc.).

Unauthorized Installations – Non-state and/or unauthorized door locks, door security devices, access control equipment (mechanical or electronic), padlocks, or cabinet locks installed on campus buildings, facilities, or equipment. (Note: The University may investigate and take appropriate action as a result of all such installations.)

Unauthorized Use – Use of keys; 1) not issued to a user consistent with this SOP, or 2) to access areas without a work-related reason. (Note: The University may investigate and take appropriate action following allegations of unauthorized use of University keys or access codes.

TYPES OF KEYS AND ACCESS CODES ISSUED:

Great Grand Master keys or access codes, with a few exceptions, will permit access to the total University complexes. The issuance of Great Grand Master keys or codes is tightly controlled to maintain campus-wide security, and is based upon demonstrated need and justification due to the wide access provided by the key or code. Any request for a Great Grand Master key or code must be accompanied by a statement of justification attached to a University Key Request Form (PeopleSoft). The Key Request form must be approved by the appropriate Dean/Administrator, the Senior Director of PPM, and the Chief of Police.

Building Master keys or access codes, with a few exceptions, will permit access to an entire building. The issuance of the Building Master keys or codes is tightly controlled and is based upon demonstrated need and justification due to the wide access provided by the key. Any request for a Building Master key or code must be accompanied by a statement of justification attached to a University Key Request Form (PeopleSoft). The Key Request form must be approved by the appropriate Dean/Administrator and the Senior Director of PPM.

Area/Department Master keys or access codes will permit access to certain areas of a building. The issuance of an Area/Department key or code is tightly controlled and is based upon demonstrated need and justification due to the wide access provided by the key or code. In order to demonstrate need, any request for a Building Master key or code must be accompanied by a statement of justification attached to a University Key Request Form (PeopleSoft). The Key Request form must be approved by the appropriate Dean/Administrator and the Senior Director of PPM.

Office keys or access codes will permit access to a specific room or rooms only (office, classroom, building entrance). Issuance of these keys or codes should be based on a need to access a specific room or set of rooms. Requests and approvals for these keys or codes must be made on a University Key Request form (PeopleSoft). The Key Request form must be approved by an appropriate Dean, Administrator, or Director.

Miscellaneous keys or access codes will permit access to items such as vehicles/carts and locking devices (cabinets, desks, etc.). Issuance of these keys or codes should be based on a need to access the specific item. Requests and approvals for these keys or codes must be made on a University Key Request form (PeopleSoft). The Key Request form must be approved by an appropriate Dean, Administrator, or Director.

RESPONSIBILITY

The Department of Public Safety, PPM Senior Director or designee, and appropriate area director will review and approve Key Request forms for keys and/or access codes.

Administrative Officers will:

- Review and approve Key Request forms for all building master, area master, entrance door and miscellaneous keys for their areas, including room(s), equipment, cabinet keys, etc. Review and approve Access Codes for building entrance and interior doors for administrative offices and labs.
- Control and limit access, whenever possible, to hazardous material storage areas.
- Ensure that all faculty and staff pick-up and return all keys to PPM.

The PPM Lock Shop will:

- Maintain databases of keys, key holders, access codes and access code holders.
- Review all Key Request forms for duplication and discrepancies and notify the administrative officer and/or requestor of such.
- Process Key Request forms signed by only those administrative officers authorized to approve key requests.

- Verify whether or not keys have been returned upon the separation of anyone having received a key.

- Remove access codes upon the separation of anyone having received an access code as reported by the administrative officer.

- Cut all university keys and install and maintain lock and access devices as authorized.

- Repair and/or replace any bent, broken or worn keys.

- Annually audit all PHYSICAL PLANT MANAGEMENT managed Omni and Sargent access control systems against separated employee information provided by Human Resources.

Authorized Key and Access Code Holders will:

- Keep key(s) and Access Codes private and in their custody at all times.

- Never transfer or allow use of keys or Access Codes unless authorized to do so by the responsible administrative officer.

- Report lost or stolen keys immediately to the appropriate administrative officer, the Department of Public Safety and PPM. If keys were stolen off campus, provide a copy of governing agency police report number.

- Return keys to PPM on the day of transfer to another department or separation from the University.

- Requesting Departments will consult with PPM as necessary prior to preparing PeopleSoft Key Request forms, obtain appropriate approvals and submit PeopleSoft requisition forms to PPM.

- Auxiliary Organizations (including the University Student Union (USU) and Student Housing) will operate and maintain a separate key control system and provide access keys and codes to university personnel for safety and security purposes.

- Contractors (in cases when contractors are issued State keys) will acknowledge responsibility for all expenses incurred by CSUN in the case of a lost key.

PROCEDURES

General procedures are as follows:

Key Issue and Return

1. The administrative officer or requesting department will submit a PeopleSoft Key Requisition form to PPM. The request shall include the building name, room number and employee ID Number.

2. Keys will be made and issued to faculty and staff who currently are employed at CSUN (state employees) and University Corporation (TUC) employees.

3. The PPM Lock Shop will maintain and update records for the key/access databases.

4. The authorized key holder, with a valid identification (CSUN ID, driver's license, etc.) will pick up the keys at PPM.

5. The authorized key holder will return all university keys to PPM on the day of separation from the University or transfer to another department.

6. PPM will verify that the keys listed in the key control database have been returned by the faculty and staff and sign the Separation form (OHRS 30- 23 dated 10/2017).

Access Code Issue

1. The administrative officer or requesting department will submit a PeopleSoft Key Requisition form to PPM. The request shall include the building name, room number and employee ID Number.

2. Access Codes will be made and issued to faculty and staff who currently are employed at CSUN (state employees) and University Corporation (TUC) employees.

3. The PPM Lock Shop will maintain and update records for the key/access databases.

4. The authorized Access Code holder, with a valid identification (CSUN ID, driver's license, etc.) will pick up the Access Code.

5. The PPM Lock Shop will remove access codes upon the separation of anyone having received an access code as reported by the administrative officer and annually audit all PHYSICAL PLANT MANAGEMENT managed Omni and Sargent access control systems against separated employee information provided by Human Resources.

Key Replacement and Facility Rekeying

1. Lost or stolen keys must be reported immediately to the Department of Public Safety, the appropriate administrative office, and PPM.

2. The department/unit administrator, in consultation with PPM and the Department of Public Safety will determine if rekeying is necessary. The cost of any rekeying will be charged to the department/unit responsible.

REFERENCES

None.

APPROVED _____ 01-31-19

Jason R. Wang, Senior Director — Date