Administration and Finance
Operations Detail: Facilities Planning & Management - 14

ADMINISTRATION & FINANCE | FACILITIES PLANNING & MANAGEMENT

Key Issuance and Control

May 2023

1.0 PURPOSE

The aim of this operational detail is to set forth guidelines and procedures for the issuance, control, and management of keys within the organization. This policy aims to ensure the security of physical assets, restrict access to authorized personnel, and prevent unauthorized entry to sensitive areas.

This operations detail is in alignment with Campus Strategic Plan Initiative 5, Objective 5.

2.0 BACKGROUND

Key issuance and control are integral components of security and access management. This encompasses the procedures for providing physical keys, card access, or other means of access to authorized individuals, all the while maintaining rigorous control and accountability measures. This operations detail outlines the process for key issuance and control utilizing the key management system, Web TMA.

3.0 OVERVIEW

The authority to request keys resides with the approving authority of each unit. Following approval, designated key desk personnel shall review and process each request accordingly. Each key is uniquely identified and recorded in the key management system (Web TMA).

4.0 CITATIONS

California Penal Code, Title 13, Chapter 3, § 469

Education Code, Title 2, Chapter 5, § 45100 - 45139

CSU Information Security Policy and Standards, IV.C.1.Personnel Information Security Activities

Information Security Responsible Use Policy, I.D.2. Responsible Use of Information Assets

Cal Poly Pomona Strategic Plan 2017-2025

Procedures for Key Issuance and Control

Facilities Planning and Management Key Request Form

5.0 PROCEDURES

Level of Keys

The "level of keys" is the hierarchy or categorization of keys based on their access privileges and the areas they provide access to. Various levels of keys are issued to individuals based on their roles and responsibilities. Key levels are as follows:

- *Individual Keys:* Individual keys provide access only to specific rooms and offices assigned to an individual. These keys are commonly issued to employees for their personal workspace.
- *Sub-Master Keys*: Sub-master keys provide access to a specific group of areas. They are issued to individuals responsible for those areas.
- *Master Keys*: Master keys provide access to a larger set of areas or departments than a sub-master key but not as extensive as a great grand master key.
- *Great Grand Master Keys*: Master keys grants access to all or most areas within a facility or building (excluding special locks). These keys are usually held by authorized personnel with the highest level of responsibility, such as facilities workers or security officers.

Single Keyed Different (SKD)

SKD are restricted keys with limited distribution and are often used for sensitive or secured areas. The following areas/departments are considered high risk or high security areas:

- University Police Department
- Cashier's Office
- Pharmacy
- Chemical/hazardous materials
- High Voltage areas
- Medical/personnel records
- University's server room

Approving Authority

The approving authority, responsible for reviewing and granting access to specific areas, contributes to an additional layer of security by ensuring that only authorized personnel can enter designated areas. The designated approving authority is as follows:

- *The University President* serves as the approving authority for great grand master keys, granting the highest level of access to multiple buildings and spaces throughout the university.
- *Divisional Vice Presidents* hold the authority to approve building master, department master, and SKD keys that access buildings assigned to their unit/division.
- *College Deans and Administrative Heads* act as the approving authority for individual room, building master, and SKD keys, providing access to rooms and building assigned to their respective college or administrative unit.
- *The Director of Student Health Center* holds the authority to approve SKD keys, granting access to the Student Health Center and Pharmacy located in Building 46.

Key Request & Issuance

The individual or department seeking access to a specific area or building initiates the process by submitting a key request form. The form should include the requester's name, department,

bronco ID, specific areas they need access to, and any required approvals. Once the key request is approved, a facilities management key desk team member proceeds with the key issuance. They will provide the requester with the necessary keys for the approved areas.

The key request form can be found on the Facilities Planning and Management website. Authorized Key Request Forms must be submitted to the key desk via email at fmkeydesk@cpp.edu, or by fax at (909) 869-4363.

The individual for whom a key is requested is responsible for retrieving the key from the key desk and must sign for the key(s) during the time of pickup. Key distribution is in building 81, room 109.

Request to SKD (Single Keyed Different) an Office/Other Space

To initiate a lock change to SKD, a written request, accompanied by a justification, must be submitted. Prior to submitting a request, the requester must obtain approval from the Dean or AVP of their college/department. SKD spaces are not integrated into the master key system, preventing UPD, Facilities, IT, and all other units from accessing the space during an emergency. The AVP of Facilities Planning & Management will assess the need to rekey the space as an SKD and authorize or deny the request.

Custody of Keys

The individual receiving and signing for a key assumes exclusive responsibility for its safekeeping and is not permitted to lend or give the key to any other person. University keys are considered state property and should not be replicated or duplicated. Individuals who duplicate keys without authorization are guilty of a misdemeanor under State law (California Penal Code § 469).

Departmental representatives entrusted with SKD keys are obligated to be accessible in situations requiring emergency access. In the event that UPD or FPM cannot reach the individuals holding SKD keys, leading to the necessity of forcible entry into a building or room, the responsible department will be accountable for any associated costs related to damage or repairs.

Key Replacement & Maintenance

In the event of lost or damaged keys, facilities management personnel have a process in place to replace keys while ensuring the security of the affected areas is not compromised. As soon as the lost key is noticed, the individual who lost the key should immediately inform their designated authority. The individual is required to complete a lost key memo, providing details about the lost key and any relevant information regarding the loss. Damaged keys will be replaced, or appropriate access control measures may be completed to prevent unauthorized access.

Key Return

The requester is responsible for using the keys responsibly and returning them promptly when no longer needed or when they leave their current role and/or organization.

Keys must be returned to the FPM key desk when the following events occur:

- *Change of Appointment*: When a change in an employee's appointment occurs, the approving authority must identify any keys to be returned and notify the key desk. All inquiries related to keys held or key returns can be directed to fmcustomer@cpp.edu.
- *Employee Separation*: Prior to an employee separating from campus, the approving authority must identify any keys to be returned and notify the key desk. In addition, employee separation summaries must be provided by Human Resources monthly. Key desk personnel shall update CMMS key records to ensure key holder profiles match the separation report.
- *Change of Lock*: When the lock to a room or building is changed, the approving authority must identify any keys to be returned and notify the key desk. In cases where a lost key poses a significant security risk, the affected locks may need to be rekeyed or replaced entirely to ensure the compromised key cannot be used to gain unauthorized access.

Violation of Policy

Individuals who fail to adhere to the policies and procedures outlined in this operations detail may be subject to corrective and disciplinary action including, but not limited to a loss of the right to be issued keys. Corrective and disciplinary action will be administered in a manner consistent with the terms of the applicable collective bargaining agreement in accordance with the provisions of the California Education Code.

Audits & Record Keeping

The primary purpose of a key audit is to assess the security of keys to identify potential vulnerabilities an ensure compliance with established policies. The FPM key desk conducts annual key audits to ensure adherence to key issuance and control policies and procedures. Key desk personnel will generate an inventory list of all keys held by a department, including keyholder and key information. The report is issued to the department head and authorized personnel is required to physically inspect and verify keys' existence and document the findings, noting any discrepancies. Upon audit completion, the findings should be reported to the key desk and records are updated accordingly.

In July of each fiscal year, a thorough review of physical keys shall be conducted. Key desk personnel shall perform a physical key count. Keys that are not accounted for are recorded on a key inventory spreadsheet. All missing SKD (Single Keyed Different), Great Grand Master and Master keys shall be reported to the FPM Manager of Projects, Maintenance & Fleet Services.

This immediate notification allows the University to take appropriate steps to protect the safety of building occupants and to secure university property. The Manager of Projects, Maintenance & Fleet Services will assess the risk to the campus and determine if the re-keying of locks is necessary. If FPM determines that a new lock or re-keying of old locks is required, the cost will be billed to the department or administrative unit that authorized the issuance of the key(s). If the key is found and returned before the locks have been replaced or re-keyed, there will be no charge.

6.0 DEFINITIONS

FPM Key Vault
The FPM key vault is a secure, centralized location designated to securely store keys.

Approving Authority
The approving authority is an individual responsible for granting authorization and oversight of keys.

SKD (Single Keyed Different) Keys
SKD are physical keys that access a single designated area (high risk or secured area).

7.0 CONTACTS

This operations detail is owned, administered, interpreted, and revised as necessary by Facilities Planning & Management.

Erica Stolz
Customer Service Center/Key Desk
Administrative Support Cord.
909-869-3387
esstolz@cpp.edu

FPM Customer Service Team
909-869-3030
fmcustomer@cpp.edu

8.0 REVISION TRACKING

Revision History

Revision Date	Revised by	Summary of Revision	Section(s) Revised
05/1/23	Jeffrey Beal Sr.	Initial Draft	All
05/26/23	Natalie Schroeder	Revised/Edited for Clarity	All

Review/Approval History

Revision Date	Reviewed by	Summary of Revision	Section(s) Revised
08/02/23	Vanessa Garcia	Final Draft	All
02/01/24	Tiffany Frontino	Final Draft	-
02/01/24	Matthew Whinery	Final Draft	-