# Facility Operations keyed lock management guidelines

The University has, at considerable expense, transitioned all DePaul-owned facilities to a new, patented master key system whereby key blanks for University doors are proprietary and are not available for sale at any local hardware store, locksmith shop or any online retailer. This means that, so long as the University controls which keys it distributes and to whom those keys are distributed, access to our facilities may be reasonably limited to only authorized individuals, without fear of illegally duplicated keys compromising the integrity of the system.

Specific guidelines for the management of keyed locks include the following:

- The assigned facility access manager must maintain a logbook, Excel workbook or Access database which clearly documents all door keys assigned to the department, area, or college. The logbook, spreadsheet or database must record who has which specific keys and must also contain an accounting for all spare keys in inventory. Though not a strict requirement, facility access managers are encouraged to document sundry keys (for file cabinets, display cases, etc.) in a similar fashion.

- The key tracking logbook, spreadsheet or database must be reviewed at least quarterly toward ensuring that all keys are accounted for and that keys are collected from those no longer requiring access to a given space. The logbook, spreadsheet or database must also be appropriately modified anytime new keys are added to inventory, anytime keys are assigned to new personnel or anytime keys are turned in due to employee turnover, completion of a project, etc.

- At the time of the quarterly key review, the assigned facility access manager must select a representative sample of departmental employees and verify that all keys assigned to those employees are in-fact in their possession and physically accounted for. Ideally, the facility access manager will verify possession of every employee’s keys at least once during the course of a calendar year.

- It is an unacceptable practice for any key higher than an office-suite sub-master to be taken off campus by any employee on a regular basis. Individuals with access to high-level keys, must secure those keys in a locked cabinet, locker, or key box prior to departing campus for the day. High-level keys should only be removed from the secured location when their use is required and they should be promptly returned to the secured location when no longer needed. Individuals with access to high-level keys should request “take home” keys from Facility Operations. Take home keys are configured to provide bare-minimum access such that the authorized person can gain entry to their workspace and access their secured key box, cabinet or locker, as needed. The idea being that a lost key ring, which provides access to a small handful of secured spaces, is less dangerous and costly than a lost key ring which provides access to many secured spaces.

- Facility access managers assigned to oversee keys are required to properly secure and organize any extra or unassigned key inventory in an appropriately locked key box, or file drawer located inside a secured office or storage room. Keys must be checked into and out of the key box or drawer as they are collected from those no longer needing them and as they loaned or assigned to others in need.

- Facility Operations only tracks who the initial requestor of a key was; it does not track who ultimately has which keys or who has access to which doors. The reason for this is that departments, areas, or colleges may collect keys from one individual and reassign the same keys to another individual, as merited by their need for access. For this reason, it is the responsibility of the assigned facility access manager to ensure that accurate records are maintained for all keys issued throughout the department, area, or college.

- Each department, area, or college must have a process in place for collecting keys from departing employees and for ensuring that those keys are promptly delivered to the assigned facility access manager to be checked into the proper key box or key drawer until they are issued to the next employee.

- In the event that a department, area, or college fails to collect all door keys from departing employees, or in the case of lost or stolen door keys, the assigned facility access manager must make an informed decision as to whether or not lock changes are required. In these instances, the protocol would be to contact Public Safety and explain the exact circumstance as to who left, what happened and what keys are now missing. Should Public Safety deem a lock change as necessary, the assigned facility access manager should call their respective Facility Operations Office and report the situation. Immediately after calling Facility Operations, the assigned facility access manager must follow up by submitting a pre-approved work order outlining which locks to change and how many new keys to issue and Facility Operations will attend to the situation promptly. Note: Departments, areas, and colleges are responsible for paying for all costs associated with lock changes and cutting of new keys.

- Broken, bent and defective keys are a security risk. Never discard broken, bent or defective keys in the trash or recycling can. All such keys must be turned over to the assigned facility access manager, who will then order replacement keys as needed. Facility access managers must return all broken, bent and defective keys to the Facility Operations Office, when going to sign for and pick up their replacement keys.

- In the event that a threat is made against a department or person by an individual with University door keys in their possession, the assigned facility access manager, or other responsible party, must promptly contact Public Safety and apprize them of the situation. If warranted, Public Safety may then contact Facility Operations and order an emergency lock change toward securing the space until the threat has been resolved.

- All requests for lock changes and additional keys must be submitted by the assigned facility access manager. Requests placed by others will be rejected. The process for requesting keys is as follows:

    - All requests for keys are submitted by the facility access manager through the Work Order System at https://fosystems.depaul.edu/metastorm/default.aspx. It is advisable to pre-approve all charges for faster service. If charges are not pre-approved, an estimate will be routed back to the facility access manager for approval prior to any work commencing.

    - The Facility Operations locksmith will verify that the person requesting keys is in-fact an approved facility access manager with key privileges. Any inappropriate or questionable requests will be declined with comments in the work order system seeking clarification or additional authorization prior to keys being cut.

    - The locksmith will deliver all new keys to the respective Facility Operations Office. The locksmith will staple a copy of the work order to the key envelope and give all key envelopes to the Facility Operations receptionist.

    - The Facility Operations receptionist will email the facility access manager, who requested the keys, and notify them that their keys are ready for pick-up.

- The facility access manager must pick-up and sign for all requested keys in person and must present a valid DePaul University ID card to the Facility Operations receptionist before the keys will be issued. The only exception to this rule is that, in the event that the requesting facility access manager is unable to pick up keys within a reasonable timeframe (due to termination, leave, or other prolonged circumstance), the person who delegated facility access management privileges to the absent individual may contact Facility Operations and make arrangements to pick up the keys on the behalf of the absent employee. For example: Should a business manager, with facility access management key privileges, order keys and then depart on medical leave, the director, who delegated privileges to them, may then make arrangements to pick up the keys in their place.

- If, after two weeks, keys have not been picked-up, a reminder e-mail will be sent to the facility access manager who requested them. After three weeks, a second reminder email will be sent to the facility access manager stating they have one week to pick up their keys. The Facility Operations receptionist will return any keys remaining after four weeks to the locksmith. All keys returned to the locksmith will be destroyed and any needed replacement keys will require generation of a new work order.

Additional guidelines pertaining to the work orders for keys are as follows:

- All costs associated with cutting of new or replacement keys, lock changes, purchasing and installing key cabinets, or other key-control devices, are the responsibility of the requesting department, area, or college and will be charged back accordingly. Any defective keys, due to lock shop error, will be replaced at no charge so long as the defective keys are returned to Facility Operations.

- In the event of new construction, floor build-out, remodeling or large-scale departmental move, the assigned facility access manager for the affected area must work with the designated representative from Facility Operations or Project Management to determine the most appropriate method for returning discontinued keys and for requesting keys to new spaces. Do not place work orders for these services without first establishing an agreeable plan with the construction project manager.

- Facility Operations work orders must be placed for the appropriate campus. A key for a Loop space for example, must be requested from Loop Facility Operations and must be picked up by the facility access manager at the Loop Facility Operations Office. Under no circumstance will keys be mailed or otherwise shipped between Lincoln Park and Loop Campuses.

- Facility access managers responsible for space in the 55E. Jackson Building should submit work orders to Loop Facility Operations for all key and lock change requests. Facility Operations will in-turn coordinate all needed work with Marc Realty on your behalf. All keys made for 55E. Jackson will be picked up at the Loop Campus Facility Operations Office.

- Suburban campus keys are requested, distributed and tracked via a separate process managed by the campus office assistant. All requests for new keys or additional access will also be coordinated by the campus office assistant.

- Facility access managers responsible for other off-site spaces leased by the University must contact the appropriate property manager to coordinate all lock and key-related requests.

## Facility Operations combination lock management guidelines

Combination door locks are intended to be used for locations which are shared amongst too many approved users to facilitate practical assignment of keys. Effective management of combination door locks begins with understanding suitable applications for these locks. Combination door locks are best suited for two-types of access control, which are limiting access to a semi-public space and limiting access to semi-private space.

- Limiting access to semi-public space is not about securing the contents or occupants of a space so much as it is about limiting who uses the space toward ensuring availability of facilities and equipment for the designated occupant group. For example, a college may sponsor a computer laboratory for doctoral candidate use only. In this circumstance, only those approved doctoral candidate students would be given a passcode to the combination lock on the laboratory door.

- Limiting access to a semi-private space is intended to protect moderately valuable University property and resources kept storage rooms and special closets. For example, a science department may have a particular piece of lab equipment stored in a closet equipped with a combination lock. Only those faculty requiring use of the equipment, are given the passcode to the lock.

Specific guidelines for the management of combination locks include the following:

- Facility Operations does not track registered users, or any usage data for doors equipped with electronic or mechanical combination locks. It is the responsibility of the assigned facility access manager to maintain a record of all who are approved to access these spaces.

- In some scenarios, one or more general passcodes, shared amongst an approved population of users, may be acceptable. This is a common configuration for certain shared restrooms, lounges and kitchens, for example. However, in most cases, the recommended practice is to assign unique passcodes to each person utilizing the space. Typically, such unique codes are based on either EMPIL ID or Student ID numbers.

- The facility access manager must maintain a logbook, Excel workbook or Access database which clearly documents all passcodes and to whom those passcodes were provided. Likewise, in the instance of personalized passcodes, the names, ID number and passcodes for each individual user should be documented for all combination door locks. If an actual paper logbook is utilized for this purpose, it must be stored in a locked file cabinet or locked drawer. The logbook, Excel workbook or Access database must be reviewed at least quarterly, by the assigned facility access manager, to ensure that access privileges are removed for those no longer requiring them due to completion of a project or change in student or employment status.

- Changes to combination lock passcodes and/or requests to add or remove user passcodes to a given lock should be submitted via the electronic work order system. One-off requests may be explained in the body of the work order. More involved requests should be submitted as an Excel file or list attached to a work order. Facility Operations does not associate passcodes with people. In all cases, it is completely the responsibility of the assigned facility access manager to properly instruct Facility Operations as to which passcodes are to remain programmed in the combination lock and which passcodes are to be removed from the lock. Facility Operations reserves the right to charge back departments for carpenter/locksmith time related in changing and updating combination lock codes.

- Because passcodes are easily shared, and because access cannot be turned on or off remotely, or otherwise changed after hours (as it can for ID swipe cards), it must be understood that combination locks are not to be used as a primary means for personal security or to provide security for high-dollar University property. High-security circumstances require the use of appropriately configured keyed locks or swipe-card access control.

- As a general rule, combination door locks are equipped with a bypass key. Facility Operations and Public Safety personnel will be granted bypass key access to these doors, such that they can perform their respective job duties. Additionally, the facility access manager responsible for the combination lock may request a reasonable number of additional keys for issuance to select faculty or staff, if necessary.

## Public Safety Access List Guidelines

The Public Safety access list is primarily intended to provide access to spaces that may not be appropriately addressed through issuance of keys, combination lock passcodes, or card swipe authorization for a variety of reasons. The Public Safety access list is a binder located at each campus' Public Safety dispatch desk which contains access requests alphabetized by department. Requests to add or remove individuals from the access list must be submitted by assigned facility access managers. Upon presenting valid identification, Public Safety will allow those individuals noted on the list access into the specified spaces. Only those individuals noted on the access list will be allowed entry, no guests will be permitted. Specific guidelines for the management of the Public Safety access list include the following:

To grant access to secured spaces during normal building hours, assigned facility access managers must provide the following information:

- The full name of each individual to be granted access.
- A specific room number or room description of the area in which access it to be given.
- By default, access privileges are granted for one academic quarter. The assigned facility access manger must provide specific dates, or a date range, if access permission is intended to be shorter in duration.

To grant access to any space outside of normal building hours, assigned facility access managers must provide the following information:

- The full name of each individual to be granted access.
- A specific room number or room description of the area in which access it to be given.
- A short explanation as to the business or academic purpose for the after-hours access.
- Specific dates or date ranges, and approved access timeframes for after-hours access must be indicated. The after-hours access list will not be used to grant unlimited 24-hour access privileges.

Additional guidelines for access list management include:

- The Public Safety access list is only available at the Lincoln Park and Loop Campuses. Each campus' Public Safety office maintains a separate access list. Assigned facility access managers must submit all access lists (as well as edits and corrections to existing lists) in writing to the attention of the Assistant Director of Public Safety (Mike Dohm for Lincoln Park Campus and Kevin Connolly for Loop Campus).

- The Public Safety access list is discarded at the end of each academic quarter. Assigned facility access managers must submit a new, updated, list at the onset of each academic quarter to re-establish any approved access privileges.

- Any questions or inquiries as to what constitutes after-hours building access should be posed to the Assistant Director of Public Safety at your respective campus.

- The Public Safety access list is not intended to provide unlimited building access to everyone. This in mind, facility access managers should not automatically put every student, faculty or staff member in a given department or program on the Public Safety access list at the onset of each quarter. Assigned facility access managers must ensure that those who are put on the access list are students, faculty and staff needing to work in a given space for a specific business or academic purpose. Please be aware that Public Safety may request that departments, areas or colleges trim down their access lists should an excessive number of names be submitted during the course of any academic quarter.

- The Public Safety access list is not intended to serve as a backup form of access should a card swipe reader malfunction. Those who have been assigned card swipe access to a space should not be added to the Public Safety list for the same space. In the off-chance that a card reader fails after-hours, Public Safety will coordinate an appropriate response with Facility Operations and IDAdmin toward ensuring that those who need to access the afflicted space may do so.

- Assigned facility access managers are responsible for maintaining all necessary records and documentation pertaining to individuals they have placed on the Public Safety access list. Public Safety does not maintain duplicate records.

- In the event that a faculty or staff member has forgotten a personal item in their office and has not realized the situation until the building has closed for the day, they are strongly encouraged to wait until the next business day to retrieve that item. If this is not possible, the faculty or staff member may present appropriate identification and request that Public Safety grant them brief access to their office to retrieve the needed item. In this circumstance, a Public Safety officer will escort the faculty or staff member to their office and provide 1-2 minutes of supervised access for the faculty or staff member to retrieve their keys, wallet, purse or cell phone, etc. Faculty and staff are not to abuse this access privilege and request more time or refuse to leave when the officer requests them to do so. Note: In the event that a faculty or staff member has accidentally forgotten their identification in their office, they should explain the circumstance to Public Safety and must present their identification to the escorting officer immediately upon gaining access to their office.

## Information Services Card Swipe Access Guidelines

Card swipe access is typically utilized to control access to exterior doors, various types of laboratory and special-purpose spaces, and primary office suite doors. Card swipes allow facility access only to specifically approved individuals and only during specified days and times.

Every card swipe enabled door throughout the University has what is called a door plan. Door plans are the rules coded into the Blackboard control system by IDAdmin which determine the operating characteristics of swipe-enabled doors. Specifically, door plans define which department, area, or college owns the door and which hours the door will be open such that anyone can enter the space (i.e. no swipe action is necessary), which hours the door is electronically locked such that only those with swipe privileges can enter the space, and which hours the door is locked such that nobody (other than Public Safety and FO) can enter the space.

While IDAdmin is responsible for performing software coding of door plan information, it does not supervise or establish the rules which govern door plans. Rather, all door plans owned by a given department, area, or college must be actively managed by an assigned facility access manager.

Facility access managers assigned to oversee door plans are expected to utilize the online facility access management program in Campus Connection (The navigation is: Main Menu → Self Service → Facility Access Management → My Door Access Plans) to perform the following tasks:

- Add and remove access privileges for specific individuals for any door plan under their supervision.

- Verify who does and does not have access privileges for a given door plan, should any questions about access status arise.

- Request one-time changes in door plan behavior. For example, locking a door early on a given Friday, due to an office retreat.

- Request semi-permanent changes in door plan behavior. For example, modifying door plan hours from June-August to accommodate a summer-hours schedule.

- Request permanent changes in door plan behavior. For example, a computer lab that was once locked down for a specific project may be reopened for general student use, during normal building hours.

Additionally, facility access managers, assigned to manage door plans, are required to do the following:

- Keep a detailed log of those who have been granted access privileges.

- Ensure that those granted access privileges, especially those granted off-hours access privileges, have a known business or academic reason for the access.

- Ensure that those who are granted access have a regular and ongoing need for swipe card access. One time or irregular needs for access are most appropriately accommodated by utilizing the Public Safety access list.

- Verify access quarterly to ensure that access privileges are limited to only those who need it, for approved business or academic purposes, and only for the days and times they reasonably need access. This will entail completing an online verification form that confirms that the door plan privileges were reviewed and updated as necessary.

Special circumstances to be aware of:

- In the event that an emergency situation prompts the evacuation of an entire campus or the entire University, Public Safety will intervene and remotely secure swipe enabled doors as needed. Doors will remain secured for the duration of the closure or until the next business day, as appropriate. In this circumstance, facility access managers are not required to take action. Public Safety will assume full control of all card swipe-enabled doors as needed.

- To expedite and simplify door plan management, facility access managers with door plan management privileges may work with IDAdmin to establish automated processes for managing access for large groups of students, faculty and staff based on enrollment or employment status. For example, an automated plan can be created to grant all currently enrolled Law School students access to the Law Library.

- Swipe enabled doors in shared spaces have more than one owner and will consequently have more than one door plan and more than one plan manager. For example, a lounge shared by two separate areas will have two door plans supervised by their respective facility access managers. Each facility access manager is responsible for assigning appropriate access only to their respective students, faculty and staff.

- Public Safety will have final say in all proposed changes to exterior door plans. Any requests to modify exterior door plans or hours must be submitted via the online system in Campus Connection; IDAdmin will then seek approval from Public Safety before any changes are processed.

- Should a facility access manager need help in determining if someone has utilized a card swipe to access a restricted area, they should send an email request to IDAdmin@depaul.edu or contact the Technology Support Center (TSC) at x28765 or tsc@depaul.edu. Note: An email to IDAdmin or a call to the TSC will result in a ticket being created. Once the ticket has been created, an IS technician will contact you to follow up on the request.

- If a facility access manager would like a new card reader installed, they should refer to the card reader installation information posted the IS web site.

- Door plan management privileges indicate which departments, areas or colleges are responsible for maintaining access control to the corresponding door. Regardless of who funded the initial installation, all doors throughout the Lincoln Park and Loop Campuses are physically owned and maintained by Facility Operations. All card swipe readers and related equipment in all University facilities are considered owned by Facility Operations and maintained by Information Services. Accordingly, all requested changes to the physical configuration of doors and card swipe equipment must be approved by Facility Operations and Information Services, as appropriate.

- All appropriate Public Safety, Facility Operations, and Information Services maintenance personnel receive access to swipe card enabled doors by means of special-purpose door plans. These areas manage their own door plans and do not require that access be assigned by any other department, area, or college. These special-purpose access plans will be appropriately administered, in accordance with these guidelines, by their respective owners.

- All door plans, utilized by Student Housing, to assign access privileges to on- campus residents are outside the scope of these guidelines and will be regulated by existing Student Housing policies and controlled through the existing software platform. However, Student Housing access privileges assigned to professional and student staff members, and all outside groups utilizing space in Housing-managed buildings (DePaulia and Radio DePaul, for example) must be assigned in accordance with these guidelines.