Facility Access Management

Category: Operations
Responsible Department: Facility Operations
Responsible Officer: VPs for Facility Operations and Information Services
Effective Date: 11/20/2017

Policy Summary

This policy establishes standards and expectations for managing access to University facilities, and for regulating after-hours access to facilities. This policy also defines policy violations such as unauthorized facility access and facilitation of unauthorized facility access.

Scope

This policy affects the following groups of the University:

- Entire University Community

This policy applies to all members of the University Community.

Policy

Purpose Statement

In the interest of protecting the University Community, its guests, and the security of University property, access to University facilities shall be regulated as follows:

- DePaul will strive to appropriately secure non-public spaces at all times, such that only those individuals with an approved business or educational purpose requiring use of the space, will be permitted to enter.

- Only those students, faculty, staff and approved contractors with approved business or academic needs may utilize DePaul facilities after-hours; and they may only do so when performing necessary work for the business or academic purpose assigned to them. All others are required to leave University facilities by the scheduled building closure time and may not return until the next business day.

Please Note:
Official University-sponsored special events and social functions are not considered after-hours access or otherwise regulated by this policy.

Building schedules (opening and closing times) may be viewed on the Public Safety website. Questions concerning building schedules, or what may constitute after-hours building access, may be posed to the Assistant Director of Public Safety at your respective campus location.

Departmental Requirements

Each department, functional area, or college must develop and implement appropriate access control procedures relative to all University space assigned to their responsibility. In developing and managing access control procedures, particular emphasis must be placed on ensuring that after-hours access to exterior doors and primary office suite doors is limited only to those individuals with legitimate and ongoing business or educational needs. Access privileges must be promptly modified or revoked upon fulfillment of the business or academic need, completion of the assigned project, or change in student or employment status, etc.

Each officer or proxy will serve as the primary facility access manager for all University space assigned to their responsibility. Primary facility access managers must utilize the Facility Access Management tool in Campus Connect to delegate day-to-day facility access management oversight and quarterly auditing responsibilities to one or more responsible full-time faculty, staff or operations contractor (Campus Recreation) member. Each primary facility access manager may reasonably dictate the reporting structure, the campus location assignments, and the overall number of delegate facility access managers appointed to most appropriately accommodate their operational structure and needs.

Once appointed, delegate facility access managers are responsible for managing the following controls and oversight measures:

- Keyed and Combination Door Locks: Delegate facility access managers, appointed with key/combination lock request privileges, must also be registered Facility Operations work order system users and must follow all applicable procedures and practices as outlined in the Facility Operations keyed lock management guidelines, and those outlined in the Facility Operations combination lock management guidelines.

- Public Safety Access List: Delegate facility access managers appointed with Public Safety access list privileges will review, update and modify the Public Safety access list per the established Public Safety access list management guidelines. Note: The purpose of the access list is to make accommodation for students, faculty and staff who may need occasional, intermittent, or one-time access to a facility and therefore should not be granted swipe-card or key access privileges. Access will be granted when an authorized individual contacts Public Safety and presents valid identification.

- ID Card Access: Delegate facility access managers appointed with ID card oversight privileges will utilize the Door Access Management program in Campus Connect and will follow all applicable ID Card Services access management guidelines to effectively establish management plans for swipe-enabled doors and to assign and remove ID card door access privileges for students, faculty and staff, as appropriate. The overarching expectation is that after-hours access, especially to exterior and suite-entry doors, is restricted to a limited

number of individuals requiring regular or frequent access for approved and ongoing business or academic objectives.

Additional Security Provisions

The following additional provisions apply:

- Automated reminder notices and nags will be deployed by Campus Connect to remind delegate facility access managers to perform their assigned quarterly audit functions. Additionally, automated courtesy e-mails will be sent to all primary facility access managers (VPs, deans, and proxies) asking that they perform spot checks of facility access management practices in their area toward ensuring that proper record keeping and audits are being performed.

- ID Card Services reserves the right to automatically purge access privileges for members of an ID Card Services-managed plan who no longer meet the employment or student status criteria established for that plan. For door access plans supervised by delegate facility access managers, only employee terminations that have been processed by Human Resources will be automatically purged. Delegate facility access managers are responsible for ensuring that all other access privileges under their supervision are maintained and updated as appropriate.

- ID Card Services reserves the right to seek approval from Public Safety prior to establishing or modifying any swipe access plan which includes exterior door access. Public Safety may limit or deny any such request at its sole discretion.

- Public Safety reserves the right to remotely disable swipe card access for any individual without advanced notice.

- Public Safety reserves the right to reasonably limit the number of people from each department, area or college included in the after-hours access list. Public Safety also reserves the right to revoke after-hours access list privileges for any individual.

- Public Safety reserves the right to remove any individual from any University facility, regardless of assigned access privileges.

- In the event of lost or otherwise unaccounted for keys, Public Safety reserves the right to mandate that the impacted department coordinate an emergency lock change with Facility Operations. All costs associated with emergency lock changes will be the responsibility of the impacted department.

- Facility Operations reserves the right to reasonably deny any key request.

Please Note:
Should a request for access be denied, the requesting facility access manager will be notified as to the reason why to the extent possible. Concerns pertaining to denied requests for access should be made to the attention of the appropriate director of Public Safety, or Facility Operations.

Violations

Obtaining unauthorized access to University facilities is a violation of University policy. This includes, but is not limited to:

- Accessing any secured spaces not assigned or authorized for use.
- Accessing any University facility outside of normal building hours, without prior after-hours access authorization.
- Accessing any space, at any time, for purposes other than the intended business or educational use of the space.
- Utilizing keys, access cards or other means to access a facility which has been closed due to an emergency situation or scheduled facility maintenance project.

Facilitation of unauthorized access to University facilities is also a violation of University policy. Facilitation of unauthorized access may include, but is not limited to:

- Loaning of keys or ID cards to grant access to an unauthorized person.
- Requesting ID card or key access for someone who is not authorized to use the space.
- Modifying ID swipe card access privileges to grant a person more access than required to fulfill an approved business or educational need.
- Sharing combination lock codes with an unauthorized person.
- Unlocking, propping, holding open, or otherwise bypassing a secured door such that it can be utilized by an unauthorized person.
- Making unofficial copies of any University key or identification card.
- Failure to promptly collect keys and access cards when required; such as upon completion of an assigned project or upon a change in student or employment status.
- Failure to promptly report lost or stolen access cards and keys to Public Safety.

Please Note:
This policy is not intended to preclude or supersede the Campus Emergency Operations Plan (CEOP). Any reasonable emergency access necessary to fulfill requirements documented in the CEOP shall not be considered a violation of this policy.

All known or suspected violations of the facility access policy must be promptly reported to Public Safety. Violations of University policy may subsequently be referred to the Associate Vice President for Student Advocacy and Community Affairs, Academic Affairs, and/or Human Resources, as appropriate. Violations may result in appropriate disciplinary measures.

Procedures

None

Divisional Collaborations

Information Services
Public Safety

Facility Operations
University Departments

Contact Information

Facility Operations
Robert Janis, Vice President for Facility Operations
bjanis@depaul.edu
(312) 362-8762

Information Services
Bob McCormick, Vice President for Information Services
bmccormi@depaul.edu
(312) 362-6627

Appendices

APPENDIX A: Identification Card Administration

APPENDIX B: Lost/Stolen Keys-Related Costs

History/Revisions

Origination Date: 01/01/2015
Last Amended Date: 11/20/2017
Next Review Date: N/A