UNIVERSITY OF SAN FRANCISCO

CHANGE THE WORLD FROM HERE

2130 Fulton Street – San Francisco CA 94117 – (415) 422-5555

CAMPUS SECURITY GUIDELINES

7/16/2009

Amended May 7, 2019

Prepared By
David Rickerson, CCCA, PSP
Project Manager, SafirRosetti
388 17th Street Suite 230
Oakland CA 94612

SafirRosetti
Security • Investigations • Intelligence
Part of GlobalOptions Group
Formerly On Line Consulting Services

TABLE OF CONTENTS

SECTION ONE

INTRODUCTION

This document provides Campus Security Guidelines for the University of San Francisco ("USF", "the University").

This document provides valuable information to the campus community of students, faculty, staff and authorized visitors on how to best contribute to the safety and security of the campus environment.

OBJECTIVES

- Develop a robust culture of security awareness amongst the USF campus community.
- Foster a sense of personal responsibility and accountability for conformance to and support of campus security measures. The USF campus community should feel empowered to act in stewardship of their campus environment.
- Encourage adherence to campus security policies and procedures to reduce or eliminate instances of circumventing controls for the sake of convenience. For example, not propping doors open, leaving exterior windows open, disabling local sounder exit alarms, or leaving personal items unattended.
- Establish clear, consistent guidelines for the allocation of campus security resources, in alignment with University priorities and applicable best practices.

CAMPUS SECURITY PROGRAM

Campus security consists of those measures designed to safeguard students, faculty, staff and authorized visitors; to prevent unauthorized access to equipment, installations, material and documents; and to safeguard them against inappropriate use, damage and theft.

"People are the most important part of any security program."

Campus security is achieved through a comprehensive integrated security program. Refer to Figure 1. A security program is "integrated" because it consists of multiple mutually supporting elements acting in concert. These elements are operational, architectural, and technological.

- Operational elements are the guidelines, policies, procedures, staffing and training that are developed, carried out and supported by people. People are the most important part of any security program. It is for the benefit and protection of the campus community that security measures are enacted, and it is through the actions of the campus community that security measures are executed.
- Architectural elements include walls, doors, roofs, windows, fences, gates, landscaping and lighting. These are the elements of the environment constructed to provide the facilities in which the campus community conducts its teaching, learning, research, and service activities.
- Technological elements are electronic devices and systems such as card swipe readers, CCTV cameras and intrusion alarm panel "burglar alarm" systems. These elements rely on the architectural and operational elements to be effective.

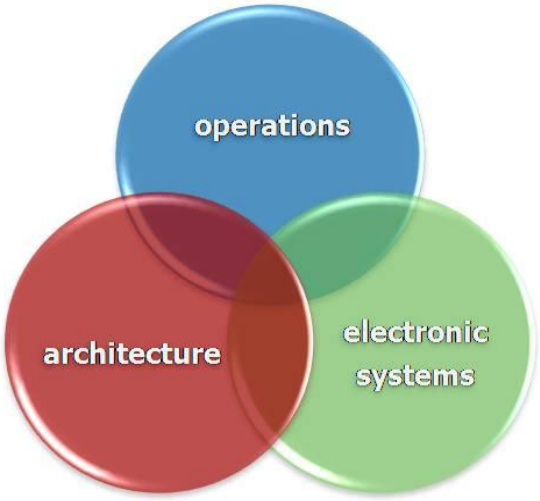

Figure 1: Security Program Elements

The operational element of the campus security program is introduced below with a discussion of the Department of Public Safety. The architectural and technological elements will be explored in greater detail in Section Two and Section Three of this document.

DEPARTMENT OF PUBLIC SAFETY

The University of San Francisco Department of Public Safety (DPS) represents half of the operational element of the campus security program. The campus community itself represents the other half, which is covered in greater detail in Section Two of this document.

Campus safety and security is most effective when students, faculty, staff and authorized visitors acting in stewardship of their campus environment work closely and communicate effectively with DPS personnel.

USF Campus Security Guidelines

The Department of Public Safety provides a variety of law enforcement and related services as well as ongoing programs in disaster, crime and fire prevention on and around the 55-acre hilltop on campus. Officers patrol campus 24 hours a day on foot, in marked vehicles, and using Segways, mountain bikes, and motorcycles. An on-campus radio communication system links Regular, Reserve, and Community Service Officers with the Public Safety Dispatch Center.

Department of Public Safety Staff

- Full-time uniformed Regular Public Safety Officers. These are armed officers in uniforms similar to the San Francisco Police Department who are responsible for continuous patrol of the University campus, initial response to campus emergencies (including medical and criminal), and the enforcement of University rules, and applicable criminal laws on campus. Officers enforce parking laws on campus, arrest offenders and provide a variety of service functions.
- Part-time uniformed Reserve Public Safety Officers. These are armed officers many of whom work for other police agencies. These Reserve Officers have the same training and duties as full time Public Safety Officers.
- Full-time and part-time uniformed Community Service Officers. These are unarmed officers in light blue shirts who enforce campus parking codes, work special events, and observe and report suspicious incidents on campus.
- Full-time and part-time dispatchers. These are University staff that work along with call takers in the Public Safety Dispatch Center in Lone Mountain as the vital communication link between the campus community and DPS personnel.

The University staffs a minimum of two (2) Public Safety Officers and one (1) dispatcher 24/7, with most shifts staffing three (3) Public Safety Officers.

All Public Safety Officers have completed a California accredited police academy. Many Reserve Public Safety Officers are active in other police departments. Uniformed Public Safety Officers have full arrest powers on duty per a memorandum of understanding with the San Francisco Police Department.

Department of Public Safety Online

Additional information may be found by accessing the USF website at http://www.usfca.edu/public_safety/ or by selecting " Student Life… Public Safety & Transportation" from the USF website homepage. Information available online includes Crime Prevention and Statistics, Public Safety News, and Timely Warnings as well as Emergency Preparedness, Parking, Safety and Transportation News.

In an Emergency Dial:

2911 from a campus phone

415-422-2911 from a cell phone

Department of Public Safety Contact Information

For non-emergency communication please call the Public Safety Dispatch Center at (415) 422-4201. For all emergency communication including fire, life safety and health emergencies please call USF Department of Public Safety immediately at (415) 422-2911.

SCOPE OF DOCUMENT

The scope of this document includes the contiguous University leased or owned property listed in Appendix 'A' of these Campus Security Guidelines.

RELATED DOCUMENTS AND REFERENCES

- DOOR LOCKS AND KEYING POLICY: Issuance and distribution of keys shall be limited and shall be in accordance with the USF Facilities Management Key Management Policy.
- STUDENT APPROPRIATE CONDUCT POLICY: Please reference the Fogcutter Student Handbook on Student Conduct, University Standards, Policies, and Procedures at http://www.usfca.edu/fogcutter/studentconduct/ and Section 05 for Prohibited Conduct at http://www.usfca.edu/Student_Conduct/Fogcutter/Section_5__Student_Conduct_Code_Prohibited_Conduct/.
- HAZARDOUS MATERIALS POLICY: Hazardous materials shall be handled and stored with the utmost care in accordance with the USF Facilities Management Hazardous Materials Policy.
- ONE CARD ACCESS AND ALARM CODE ISSUANCE POLICY: Issuance and distribution of One Cards and alarm codes shall be in accordance with the USF One Card Access and Alarm Code Issuance Policy. Please reference http://www.usfca.edu/onecard/access/

APPROVAL AND AUTHORITY FOR THIS DOCUMENT

These Campus Security Guidelines have been developed by the Campus Security Steering Committee in association with the Campus Security Subcommittee and approved by the President's Cabinet. The Campus Security Steering Committee is comprised of the Senior Director of Public Safety, the Vice President of ITS, and the Assistant Vice President of Facilities. The Campus Security Subcommittee is comprised of practitioners from Public Safety, ITS, Facilities, SHaRE and Special Projects.

Revisions, clarifications and additions to these Campus Security Guidelines may be appended to the document in Appendix 'B' by the Campus Security Steering Committee.

SECTION TWO

BUILDING HOURS

All USF buildings have the same standard building hours schedule. Building entry doors will be opened at 7:00 AM and closed at 8:00 PM. Building hours may be more restrictive than the standard building hours schedule based on a building access control manager's request.

Campus buildings are open from 7 AM till 8 PM.
After hours, just use your One Card!

Between the weekday hours of 8:00 PM through 7:00 AM and between the weekend hours of 8:00 PM on Friday through 7:00 AM on Monday buildings will be accessible through the use of an authorized USF One Card. There may be certain times of the year when campus buildings are on a modified building hours schedule, but will still be accessible through the use of an authorized USF One Card.

Summer and Holiday Hours: Addendum July 2015

An analysis of crime statistics and building perimeter door access suggests a relationship between the number of hours in a day that a building's perimeter doors are freely accessible to the general public and the level of theft experienced within that building. Simply reducing the free access to a building in the evening by 3 hours each day (e.g. building requires One Card access to enter starting at 5 PM instead of 8 PM) resulted in a 40% reduction in crime/theft within that building. During the summer months at USF there is a general decrease in foot traffic within buildings, especially during the evening hours. To address these security concerns, the following "summer and holiday schedules" of door access will be implemented.

Policies:

- Summer:

Beginning on the Monday after the last spring commencement and ending on the Monday prior to Move-in Weekend, the University Center, Lone Mountain Main (front glass doors) and Lone Mountain Rossi (front doors) will be open from 9:00 AM until 5:00 PM. All other buildings will remain locked, however accessible with a valid USF one card.

- Winter break:

Beginning the day after the final winter commencement and lasting through the Monday before the first day of the Spring Semester, the University Center, Lone Mountain Main (front glass doors) and Lone Mountain Rossi (front doors) will be open from 9:00 AM until 5:00 PM. All other buildings will remain locked, however accessible with a valid USF one card. Between December 24th. and January 1st the exterior doors to all buildings will be locked, and students will have access to any university buildings. Faculty and Staff will have normal access.

- University Holidays:

All campus buildings will be locked and will require a valid USF One Card for entry.

- Other Exceptions:

Due to incidents and/or events taking place on campus or in the local area, University Officials may override the normal building schedules.

During building hours, the quantity of open entry doors at the building's perimeter should be kept to a minimum, such as main lobby entry doors only. Other building perimeter doors may allow access through the use of an authorized USF One Card and will always allow free egress from the building, but should not be left unlocked or propped open.

Prearranged exceptions to building hours can be scheduled for specific buildings, such as for special events. To request a temporary change in the building hours schedule for a specific building, a request may be submitted by logging onto the One Card Office website at http://www.usfca.edu/onecard/, clicking on the "Request Access" link in the Quick Links and then completing the form. Requests should be completed at least 48 hours in advance. If the event is being arranged through Events Management the building hours adjustment will be made by Events Management.

The appropriate executive officer or his or her designee acts as the building access control manager and is responsible for assigning card holder rights by individual card holder to specific access-controlled doors.

PROHIBITED ACTIVITIES

Some activities circumvent, diminish or otherwise weaken the campus security of the University community and are therefore prohibited.

Prohibited activities include, but are not limited to:

- Propping open of any of the following doors: doors equipped with card access controls, automatically locking doors, normally locked doors, doors with local sounder exit alarms (including Detex exit device alarms) and any building exterior perimeter door.
- Disabling automatic door closers, locking door hardware, or exit devices.
- Disabling any security device, such as CCTV cameras or local sounder exit alarms.
- Obstructing stairways, building exits, hallways and doorways.
- Locking emergency exit doors in the path of free egress travel.
- Unauthorized installation of security equipment, accessories and systems, security devices, cameras, and fake or "dummy" cameras. Please refer to the request forms and procurement process in Section Three of these Guidelines.
- Unauthorized accumulation or duplication of keys.
- Sharing of USF One Cards or keys. Using a USF One Card or key that is not your own or allowing others to use your USF One Card or key.
- Sharing of intrusion alarm panel PIN codes. Using a PIN code that is not your own or allowing others to use your PIN code.
- False activation of fire alarm manual pull stations or emergency telephones.
- Leaving exterior windows open when room is unattended, especially after building hours.
- Use of Negoesco Field and Ulrich Field/Benedetti Diamond outside of scheduled authorized times.
- Unauthorized entry to mechanical, electrical, or IT rooms.
- Unauthorized vehicle traffic on Lower Campus.

CAMPUS SECURITY ADVISORIES

The following Campus Security Advisories are general suggestions and recommendations for personal safety and situational awareness while on campus:

- Don't leave personal items unattended! It just takes a moment for your personal belongings to be stolen, but the consequences can be long lasting.

- Tailgating is when someone follows a person through an access controlled door after that person swipes their USF One Card. Holding doors open for people behind you might be the polite thing to do, but before allowing someone to follow you through an access controlled door, ask yourself "Is this person personally known to me? Do they have a USF One Card?" A polite 'may I help you?' is the best approach for challenging individuals who are entering campus buildings after building hours without using their USF One Card. Please report suspicious persons to the Department of Public Safety.
- More information including public safety tips may be found at the USF Department of Public Safety website at http://www.usfca.edu/public_safety/.

ENFORCEMENT OF THE PROHIBITED ACTIVITIES POLICY

Reporting of Misconduct If a member of the University community observes or receives a report of a violation of the Prohibited Activities Policy, that member is encouraged to notify DPS at dispatcher@usfca.edu.

The Senior Director of the Department of Public Safety will coordinate a proper incident response.

Investigation and Adjudication of Security Violations Allegations of violations of this Prohibited Activities Policy are resolved in accordance with applicable University policies and procedures. Members of the University community found responsible for violating this policy are subject to a full range of sanctions, including but not limited to the loss of campus building access privileges, suspension or expulsion from the University, and/or termination of employment. Some violations may constitute criminal offenses under applicable laws and USF may report such violations to the appropriate authorities.

USF ONE CARD POLICY

USF students, faculty, staff, contractors and USF Affiliates are issued a USF One Card by the One Card Office. For more information regarding the USF One Card please refer to the website of the USF One Card Office at http://www.usfca.edu/onecard/.

A USF One Card identifies the cardholder by name as an authorized member of the University community and can be assigned access control authorization rights. The USF One Card should be kept in your possession while on campus and available for display upon reasonable request.

SECTION THREE

SECURITY STANDARDS OVERVIEW

This section presents general design principles and concepts that guide the application and installation of security devices and systems at the University of San Francisco.

The following security design considerations apply to security projects including new construction, and remodels, and should be reviewed prior to remediation of perceived defects. Members of a project design team should refer to these design considerations as a guide for the intent and goals of security devices and systems installation.

The Campus Security Steering Committee will seek to incorporate the input of involved and affected individuals but retains final decision-making authority and control of the procurement process. These design considerations are guidelines and allow for flexibility and judgment in how the intent is satisfied through the procurement and installation of various specific devices and systems.

SECURITY DESIGN CONCEPTS

Objective

The objective of installing security devices and systems is to increase the safety and security of the campus community through the use of security controls designed to delay, detect and deter inappropriate and unauthorized conduct. Security devices and systems are the technological element of the campus security program that work with the operational and architectural elements. It is the cumulative effect of the use of security measures as part of the campus security program as well as assessment and response to inappropriate and unauthorized conduct that produces the desired effect of increasing the personal safety of the individuals that make up the campus community.

Campus security measures are further supported by various programs and initiatives managed by the Department of Public Safety:

- Education and Awareness
- Campus Resiliency Plans
- Emergency Response and Incident Management

Security Controls

The campus security design intent is to implement measures which operate as parts of an integrated system of security controls. Campus security controls act as countermeasures for vulnerabilities. There are two main types of controls:

- Preventative controls reduce the likelihood of a deliberate aggressor attempt, protect vulnerabilities, and make an aggressor attempt unsuccessful or reduce its impact. Examples of preventative controls are door locks, window latches, and card swipe readers.
- Detective controls discover aggressor attempts and activate preventative or corrective measures. Examples of detective controls are intrusion alarm panels, motion detectors, CCTV cameras, and panic buttons.

Layered Protection

Campus security controls are deployed to create layers, or concentric rings, of security. Refer to Figure 2. The layers start at the outermost boundary of the campus, and work their way in to the building exterior perimeters, restricted interior areas, and finally to the protection of assets such as computers, supplies, or lab equipment and the protection of containers such as safes or file cabinets. By inhibiting the travel of unauthorized individuals while assisting the travel of authorized individuals, security controls help protect members of the campus community at every layer.

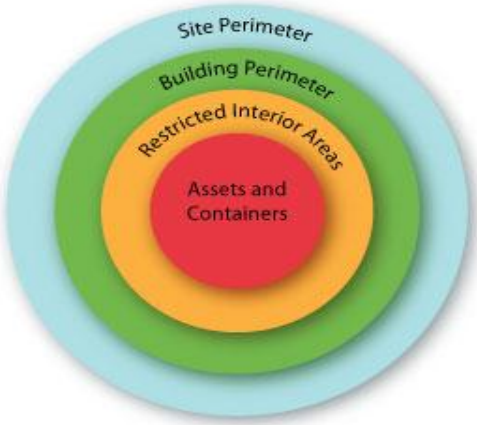

Figure 2: Layers of Security Controls

The campus site perimeter is defined by the boundary of USF's private property. Security controls are deployed at this layer to clearly indicate the transition from public to private space in order to demonstrate that this is private property which is supervised and controlled by the owner and subject to restrictions not found in public places. This definition also serves to reinforce the territoriality of the campus community over "their" campus.

A building's exterior perimeter is defined by the walls, doors, windows and roofs that form the exterior structure of the building itself. Security controls are deployed at this layer to facilitate management of the use of the building by providing the means of control over entry into the building.

Restricted Interior Areas

Restricted interior areas are defined by the nature of the activities or assets contained within. Refer to Figure 3. If a restricted interior area is determined by the nature of the activities or assets contained within, then a hierarchy of criticality of those activities or assets can be used to inform decisions about the deployment of security controls. In this hierarchy, health and human safety is first priority, then confidential and proprietary information, followed by assets such as cash or expensive equipment. If an area does not fall under this hierarchy then it should not be considered a restricted interior area.

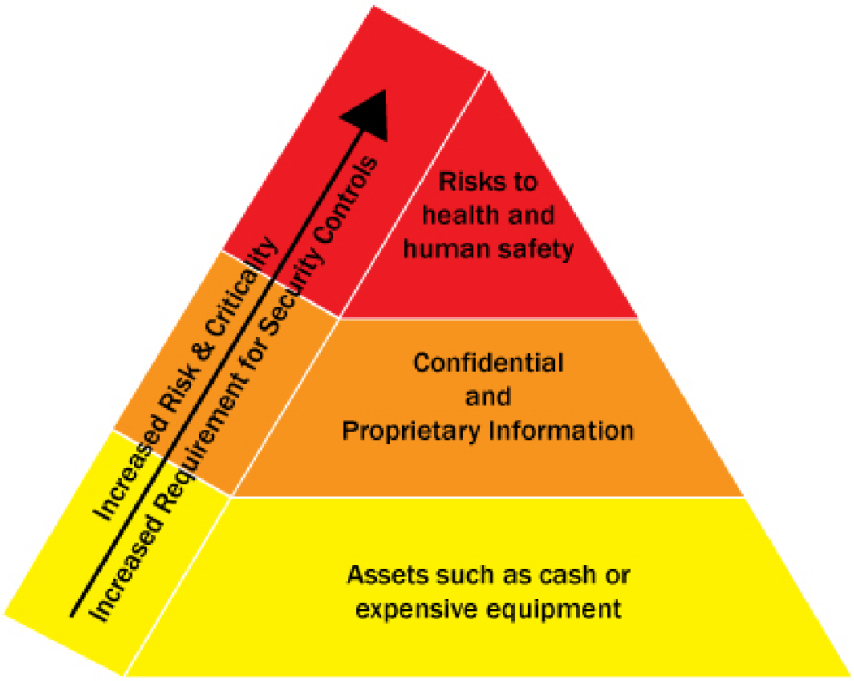

Figure 3: Hierarchy of Criticality

For example, hazardous chemical storage is a restricted interior area because of the potential for injury to persons entering the area. Offices where personnel reviews or termination may occur and the Office of Student Conduct Rights and Responsibilities are also restricted interior areas due to a different kind of risk to human health and safety. Security controls are deployed at this layer to reduce the likelihood of injury by providing the means of control over entry into the area. Additional security controls such as panic buttons in these areas provide a means of signaling the presence of risks to human health and safety directly to the Department of Public Safety.

Funneling

Focusing people's movement by funneling them toward a limited number of passageways and doorways when crossing through security layers creates identifiable transition points. These transition points are where security controls of the two types listed above (preventative and detective) can then be applied. Creating a specifically identified and limited number of transition points reduces the amount of area that needs to be covered by security controls, which in turn increases the effectiveness and efficiency of those controls.

Therefore, a person must come into repeated contact with security devices and systems to pass through the points of transition while traveling onto the campus, entering into individual buildings, entering into a specific area of a building, and then gaining access to specific assets. Security controls exist to grant access just as much as to prevent access. For authorized individuals these security devices and systems facilitate their passage, providing quick access as they go about their business. For unauthorized individuals, however, these security devices and systems restrict and detect access at each transition point.

SITE DESIGN CONSIDERATIONS

A. Campus Perimeter

1. The private property boundary of the University should be clearly identifiable. Perimeter definition can be attained through the use of multiple mutually-supporting elements such as barriers, fences, signage, lighting, landscaping, color schemes, markings, statues, street names, street markings, or curb painting.

B. Lines of Sight

1. Sight lines should be clear within the perimeter of the property along pathways and common areas between structures. Of particular concern is the nighttime line of sight from buildings toward parking areas.
2. Landscaping will be planned and maintained to promote adequate security lighting and observation. Plants are to be planted so as to not to obstruct the view of exterior CCTV cameras.

C. Concealment

1. Care should be taken to not create architectural niches or recesses in buildings and under parking structures large enough to conceal a person, unless planted with dense or thorny bushes or blocked by a barrier such as chain link fencing.
2. Shrubs and bushes planted near the building should be planned and maintained to permit security patrol observation and to discourage concealed environments.

D. Emergency Telephones

1. Emergency telephones provide a means of communication to the Department of Public Safety to convey distress and request assistance in critical situations such as criminal victimization, as well as fire, life-safety, and health related emergencies.

E. Site Lighting

1. Lighting of the exterior of buildings, common areas, pathways and parking lots should be uniform maintained lighting established to facilitate visual observation and way finding. "Uniform maintained" means evenly dispersed between light poles to avoid bright light under the pole and then darkened areas between the poles.
2. Site lighting should be installed and maintained with sufficient coverage and luminosity to support its various functions such as safety against trips and falls, illuminating foot and vehicle traffic, and for safety when walking at night.
3. Site lighting should also support CCTV video surveillance and direct visual observation.

F. Patios and Balconies

1. When there are patios or lanai on the exterior of a building or balconies on upper floors that connect two or more exterior doors or are accessible from the ground level, the doors at those patios and balconies should be considered as building exterior perimeter doors.

G. Stairs and Stairwells

1. Lighting of stairs and stairwells should be uniform maintained lighting established to facilitate safe use of the stairs. "Uniform maintained" means evenly dispersed on stairs, landings, entries and exits to avoid darkened areas in and around the stairs.
2. Exterior doors at building stairwell towers should be equipped with automatic door closers and locking door hardware to help enforce the use of stairwells in the free egress direction only. Travel between floors using stairs should be encouraged where that use is part of the building design, but even in this situation the exterior door at the ground level should automatically close and lock to help enforce the use of ground level stairwell exit doors in the free egress direction only.

H. Exterior Storage

1. Exterior storage areas that contain potentially hazardous materials should be completely enclosed and locked with chain link fence or a combination of walls and chain link fencing. The top of the enclosures should be covered to prevent unauthorized entry.

I. Perimeter Vehicle Entries and Parking

1. Bollards and barriers, one-way streets, limited entrances/exits, cul-de-sac, speed bumps, and signage should be installed to discourage through traffic and driving into unauthorized areas.
2. The interior of the Lower Campus is a pedestrian-only zone (with the exception of designated parking lots). Only authorized vehicles will be allowed access to the interior of the Lower Campus.

3. The Upper Campus has both pedestrian and vehicle use zones. Streets, parking lots, sidewalks and crosswalks should be clearly marked to keep pedestrians on sidewalks and crosswalks and out of traffic in the streets and parking lots.

J. Roofs

1. Roofs are subject to unconventional methods of building entry including ladders and fire escapes, skylights, roof doors and hatches, towers, and utilities service area entries. Roof hatches and doors that provide interior access to the roof should be latched and locked with a door lock or padlock. Authorized access to the roof should be limited by job function.
2. Skylights should be secured by their mechanical or electro-mechanical operation mechanisms and should not be left open when area is unattended.

BUILDING PERIMETER DESIGN CONSIDERATIONS

A. Entrance/Exit Lighting

1. Lighting of the exterior entries to buildings should meet or exceed the minimum standards of the surrounding exterior areas for increased visibility. Lighting at building entrances should be uniform maintained lighting to support CCTV video surveillance and direct visual observation.

B. Perimeter Doors

1. The number of building perimeter main entry doors that will remain open during building hours should be kept to a minimum, such as main lobby entry doors only. These main entry doors will be equipped with card swipe readers (for use outside of building hours).
2. Building perimeter entry doors should be monitored alarm points.
3. Other building perimeter doors may provide access through the use of card swipe readers and be a monitored alarm points, but these secondary entry doors will not remain open during building hours.
4. Building perimeter doors must always allow free egress from the building, but should not be left unlocked or propped open.
5. Doors provide a level of protection equal to the weakest part of the combination of movable parts, door material, hinges, frame and fasteners. Exterior doors should be of sufficient sturdy construction so as not to allow easy entry. Exterior out swinging door hinges should be installed with concealed hinge butts to block exterior removal of the hinge pin. Exterior doors should be equipped with commercial locksets such as Schlage or equal.
6. Interior CCTV cameras at building perimeter doors should be facing outward to capture the likeness, description and direction or travel of people entering the building.

C. Mechanical Room Doors

1. Where possible, exterior doors that provide access to mechanical rooms should lead directly into those areas rather than require travel through the common areas of the building. Mechanical room doors should be latched and locked. Authorized access to mechanical rooms should be limited by job function.

D. Emergency Exit Doors

1. Emergency exit doors should be equipped with local horn sounder exit alarms with key switch status alarm and door opened alarm in addition to being a monitored alarm point to the security system when they are part of an intrusion alarm panel zone to send a signal to Public Safety Dispatch Center if there is a security violation. These doors should remain locked from the exterior side.

E. Perimeter Windows

1. Window frames should be securely fastened so that they cannot be pried loose from the window framing. Where operable windows are installed, they should have a locking mechanism to secure them on the inside of the window and should not have outside hinges or hinges with pins that can be removed.

INTERIOR DESIGN CONSIDERATIONS

A. Interior Doors

1. Doors provide a level of protection equal to the weakest part of the combination of movable parts, door material, hinges, frame and fasteners. Interior doors should be of sufficient sturdy construction so as not to allow easy entry.
2. Doors and windows into restricted interior areas are part of an intrusion alarm panel zone and should be a monitored alarm point wired to the security system to send a signal to Public Safety Dispatch Center if there is a security violation. Restricted interior areas should be access controlled with card swipe readers and should be alarmed with a dedicated burglar alarm system with arming station keypad. These alarm points will send an alarm signal when the associated dedicated burglar alarm system is armed by use of the arming station keypad.

B. Mechanical Room Doors

1. Mechanical room doors including elevator machine room doors should be latched and locked. Authorized access to mechanical rooms should be limited by job function.

C. Interior Access Control

1. Card swipe reader access control, alarm monitoring, and communication systems (such as emergency telephones and/or entry telephones) should be installed for each building.

2. Access control systems and devices must be compatible with the security system control equipment currently installed in the Public Safety Dispatch Center. Card swipe readers, alarm inputs, and signal outputs should be controlled by these systems.
3. Access controlled doors equipped with card swipe readers should be monitored for forced door opening.

D. Interior Video Surveillance

1. Color high-resolution CCTV camera surveillance will be utilized primarily as a post incident or alarm review tool. CCTV cameras should be equipped with video motion detection and will be recorded. The recording equipment and media should be located in a secured room with the capability for review of live and recorded video.

E. Color high-resolution CCTV camera surveillance will be used to monitor floor transitions in each building.

F. Point of Sale and Cash Storage

1. Personnel responsible for cash handling, counting and storage should make arrangements with DPS for escort to cash deposit areas.
2. Cash registers and other points of sale should be equipped with CCTV camera surveillance and panic buttons at the discretion of the Campus Security Steering Committee taking into consideration factors such as volume of cash handling, level of exposure to public, and isolation from other campus activity.
3. Areas specifically used for cash storage are designated as restricted interior areas.

G. Materials Management and Shipping/Receiving Dock

1. Where possible, dock areas should be designed so that drivers can report to shipping and receiving clerks without moving through storage areas.

H. Lobby and Reception

1. Reception areas should be constructed to provide adequate viewing of the adjacent waiting areas. Obstruction, which might obscure the view of staff, such as large plants, columns, and furniture, should be avoided.

I. Residence Halls

1. Residence Hall entrance doors should have card swipe readers.
2. Residence Hall room doors should be equipped with card swipe readers.
3. Front reception desks in the Residence Halls should be equipped with CCTV camera surveillance, face recognition devices, and panic buttons.

J. Faculty Offices

1. Faculty offices should be equipped with card swipe readers.
2. Faculty offices do not require CCTV cameras, panic buttons, or a dedicated burglar alarm system with arming station keypad.

K. Classrooms and Lecture Halls

1. Classrooms and Lecture Halls should be equipped with card swipe readers.
2. Audio-visual equipment installed within classrooms and lecture halls such as overhead projectors should be secured appropriately and equipped with a monitored alarm point wired to the security system to send a signal to the Public Safety Dispatch Center if there is a security violation.

L. Library

1. Gleeson Library and Zief Law Library should follow the same principles as other campus buildings including having a limited number of main entries open during building hours, card swipe readers on building exterior perimeter doors, and alarmed emergency exit only doors. Libraries should also designate restricted interior areas as applicable and equip these areas with intrusion alarm panels, arming stations, motion detectors and alarm contacts on entry doors.
2. CCTV monitors at staffed areas should be installed to provide staff with the ability to spot check certain areas as well as provide notification to visitors that the premises are under CCTV surveillance.
3. Gleeson Library – Donohue Rare Book Room should be designated as a restricted interior area and equipped with an intrusion alarm panel, arming station, motion detectors, alarm contacts on entry doors, and CCTV cameras.
4. Library reading rooms that do not have clearly defined ingress/egress control points such as the Del Santo Reading Room in Lone Mountain Central and the Terrace Room in Zief Law Library should be equipped with CCTV cameras in support of signage that indicates the policies regarding acceptable use of the space. CCTV monitors at staffed areas should be installed to provide staff with the ability to monitor these reading rooms.

M. Executive Offices

1. Executive offices and suites are restricted interior areas due to the potential for risk to health and human safety, the increased need for access control, and the presence of sensitive and confidential files.
2. Executive offices and suites should be equipped with intrusion alarm panels, arming stations, motion detectors and alarm contacts on entry doors.
3. Executive offices and suites should be equipped with card swipe readers at the entry doors and panic buttons at the reception desk.

N. Exceptions

1. Where floors, suites, and wings of multi-use buildings are not specifically addressed in these Guidelines, the space should follow the same principles as if it was a stand-alone campus building. Theaters, for example, can be configured with limited main entries, dedicated building hours, alarmed emergency exit doors and designated restricted interior areas as applicable.

APPENDIX 'A'

The complete listing of University of San Francisco campus buildings included in these Campus Security Guidelines is as follows:

101 Howard St.
281 Masonic
Cowell Hall
Fromm Hall
Fulton House
Gillson Hall
Gleeson Library
Harney Science Center/Lo Schiavo CSI
Hayes-Healy Hall (including Facilities & Receiving and Parking Garage)
Kalmanovitz Hall
Kendrick Hall
Koret Center
Lone Mountain (including Studio Theater, Pacific, and Rossi wings)
Lone Mountain North
Loyola House (including Parking Garage)
Loyola Village (including Parking Garage)
Memorial Gymnasium
Pedro Arrupe Residence Hall
Presidio
School of Education (including USF Presentation Theater)
SOM – Malloy Hall & McLaren Conference Center
St. Anne Residence Hall
St. Ignatius Church
Toler Residence Hall
Ulrich Field – Benedetti Diamond
University Center
Zief Law Library

APPENDIX 'B'

The University of San Francisco Campus Security Steering Committee may append additional documentation or clarification to these Campus Security Guidelines in this Appendix section.

APPENDIX 'C'

Suggested requests and proposals for security technology implementations should be submitted by a building access control manager to the Senior Director of the Department of Public Safety (DPS). The Senior Director of DPS along with the Campus Security Subcommittee and the Campus Security Steering Committee will review and refine the request/proposal with regard to its requirements for scope, budget and schedule and either reject or approve the request/proposal for execution. The submitting building access control manager will be informed of the disposition of the request/proposal. **Refer to the flowchart on the following page**.

USF Campus Security Guidelines Appendix 'C'

Campus Security Services Request Procedure