LIBRARY SECURITY GUIDELINES DOCUMENT
JUNE 27, 2010

Prepared by
LLAMA BES Safety & Security of Library Buildings Committee:

Pat Wilson, Chair
Ewa Barczyk
Trisha Burns
Caryn Carr
Michael Daly
Robert Danford
Derek Dolby
Helen Henry
Michael Montgomery
Kathy A. Parsons
Laverna Saunders
Stephen Shaw
Jean Zanoni

Table of Contents

Disclaimer

The information contained in the Library Security Guidelines is for general information purposes only. The information is provided by the LLAMA BES Safety and Security of Buildings Committee and, while we endeavor to keep the information up-to-date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the Guidelines or the information contained herein. Any reliance placed on such information is strictly at ones risk.

The Committee and its members shall not be liable for any loss or damage including, without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this Security Guidelines.

Introduction

"Library Security Guidelines" is the latest in a series of documents derived from a 1989 document produced by the American Society for Industrial Security (ASIS) and revised under the auspices of the Safety and Security of Library Buildings Committee of the Buildings and Equipment Section of the Library Leadership and Management Association (LLAMA), a division of the American Library Association.

The documents that formed the basis of the current revision are:

- "Suggested Guidelines in Museum Security," AIIS Standing Committee on Museum Library and Archive Security, 1989, revised 1997.
- "Library Security Guidelines," 1996, Eric Belzer, Buena Vista University, and David Liston, Smithsonian Protection Outreach Officer.
- "Library Security Guidelines" 2001, Safety and Security Committee, Building and Equipment Section, Library Administration and Management Association (LAMA), a division of the American Library Association, Merri Hartse, chair.

The current revision is the product of the Safety and Security Committee of LLAMA BES, Elizabeth Titus (2008-09) and Pat Wilson (2009-10), chairs.

While these "Guidelines" incorporate or recommend industry standards and note best practices, the document does not attempt to establish standards and in no way implies that libraries that do not or cannot adopt the recommendations are in any way negligent.

These "Guidelines" and recommendations must be evaluated against local codes and regulations and established institutional policy and procedure. Not all aspects of all recommendations will apply to all libraries. The recommendations are voluntary and represent the composite opinion of leading experts in the field of library security.

It is clear that some libraries will not have the staff necessary to comply with some of the guidelines. Many libraries, for example, do not have a security force or a director of security and cannot hire either. But in adopting the spirit of the guidelines, these libraries can designate one person to be responsible for these duties.

Successful library security programs are based on clearly defined and well-communicated behavior policies for public and staff. Although these guidelines do not explicitly refer to "rules of conduct," the assumption is that the library has a set of rules governing public and staff conduct. Please note that these policies should be reviewed by the library's legal counsel and approved by the library's governing body.

Today, more than ever, security in your library is every staff member's responsibility. Even in libraries with a security force, officers can only be in one place at a time—it is everyone's responsibility to ensure a safe environment for the public, the staff and the collections.

Definitions

alarm monitoring facility: central station where security, fire or other emergency alarms are monitored and persons are dispatched to investigate the alarm.

assets: refers to what the library has or owns and considers valuable, including human life, collections, structures, properties, even the good name and operations of the library.

collection and objects: materials collected by libraries and archives to include but not limited to books, periodicals, manuscripts, maps and recordings.

commissioned: award of law enforcement powers to arrest and bear arms.

CPTED: Crime Prevention through Environmental Design.

disaster: uncommon, uncontrollable events such as a dangerous weather storm causing damage, sometimes contrasted with "emergency" which refers to interruptions to library operations that are relatively common, controllable emergencies such as electrical power outage, often used synonymously.

emergency: an interruption to library operations that is relatively common, controllable, contrasted with "disaster" above, but often used synonymously with it.

guideline: procedure, practice or system recommended as a minimum step toward providing protection in a library. These are not standards.

library/archives manager: operational director of the library or archives.

object or collection object: one of the materials, collected by libraries and archives, defined under "collection" above.

perimeter security: protection concept of designing a three-dimensional ring around objects of value, often one inside another, such as a property line perimeter, building shell perimeter, non public area perimeter and high value area perimeter.

policy: as used in this document is a library-wide scheme, while "program" and "plan" are management procedures for specific subjects. Specific procedures may be called "instructions," "manual," or "rules".

protection: includes physical security, fire protection and emergency planning, contrasted with "security" below, with which it is often used synonymously.

secured area: an area who perimeter security has been reviewed and usually reinforced, with entries and exits locked or under observation and generally alarmed when empty.

security: generally refers to physical security protection, but here, as elsewhere, is a common synonym for "physical protection" that includes fire protection and emergency planning.

security manager: library/archives staff person who is appointed to be responsible for library security and protection issues.

security staff: staff who have security duty to perform, when they are performing that security duty.

shall: means "critical" for compliance.

should: means "highly desirable" for suggested or recommended compliance.

special collections: refers to high value collections.

staff: any persons who can be held responsible for their actions by the library, including paid and unpaid staff, volunteers, interns, researchers, contract and maintenance workers.

staff with primary security duties: staff who are dedicated to work conduct security duties most of their working time, usually staff of a security office or security department.

Section 1. Duty to protect

The scope of this duty shall not be limited by the type, size of library, governance, or collection.

It is suggested that the Library Director, or designee in safety and security matters, should be responsible for:

1.1 ensuring the physical protection of both library staff and library patrons. He/she also is responsible for protecting the building, its contents, and its immediate surroundings. The responsibility includes, but is not limited to, the development and integration of protection programs for emergencies, as well as fire, floods, earthquakes, and other natural disasters.

1.2 ensuring that library staff are informed of and instructed in their obligations in safety and security matters, for example, the obligation to protect lives and collections, to provide aid to disaster victims, etc.

1.3 taking all reasonable steps to minimize loss and damage to collections, furniture, and equipment.

1.4 developing and integrating a library asset protection policy that addresses, as appropriate to the nature and size of the library, fire and emergency protection, described in Section 4; physical barrier and lock and key protection, described in Section 5; security staff protection, described in Section 6; personal access and parcel control protection, described in Section 7; security alarms and electronics protection, described in Section 8; crime prevention through environmental design, described in section 9.

1.5 auditing the library's assets and its protection systems on a regular basis. When possible such audits should be conducted by security professionals independent of the library with no product or service-related bias.

Section 2. Foreseeability of Loss

It is suggested that the Library Director, or designee in safety and security matters, should be responsible for:

2.1 anticipating, and taking reasonable measures to prevent predictable losses such as minor vandalism, injuries, theft of library materials or library user property, utility interruptions, and the non-return of items borrowed from the collection.

2.2 anticipating, and taking reasonable measures to mitigate catastrophic losses that occur during emergencies and natural disasters, such as earthquakes, major fires or floods, major structural, medical and chemical accidents, weather-related catastrophes, and those from civil unrest, drawing upon local and regional experience as a means of loss avoidance (see Section 4). As the library develops strategies and programs for security it should examine the experiences and responses of neighboring institutions which have dealt with some of these issues. Law enforcement, fire service, risk management, insurance professionals, and others with expertise in loss prevention also should be consulted as appropriate.

2.3 working closely with agencies responsible for recruitment and appointment of personnel to ensure that staff and professional employees have received verification of their identity and past history, avoiding, where possible, any potential threat to other staff, the public, the collections, or other building contents. See Appendix B.

2.4 documenting all losses, including those from fires, natural disasters, crimes, antisocial behavior, etc., that occur on or near the library involving library staff, library users, their property or library property. This information should be collected and organized in a manner that facilitates the anticipation and prevention of further losses.

2.5 monitoring and maintaining communication with theft reporting agencies or media, particularly electronic distribution lists dealing with library loss prevention, security, and stolen property reporting as a means of avoiding the purchase of stolen property and of keeping abreast of security trends and issues.

2.6 reporting promptly any obvious losses to appropriate institutional officials and external agencies to increase the possibility of recovery, to promote the apprehension and punishment of the perpetrator(s), and to help other libraries to avoid similar losses.

2.7 seeking professional external evaluation of any high-threat sites within the library and any collections, furnishings, or equipment with unusually high value in order to anticipate and prevent security program inadequacies.

Section 3. Adequacy of Protection

It is suggested that the Library Director, or designee in safety and security matters, should be responsible for:

3.1 managing situations of gravity and sensitivity and to provide clear and immediate or timely emergency direction.

3.2 preparing a library security policy that includes staff rules to protect people, collections, facilities and grounds, and that applies to everyone regardless of position, rank, title, status, or similar criteria.

3.3 implementing employment practices to ensure consistent and comprehensive evaluation of potential staff hires. See Appendix B.

3.4 evaluating threats against persons and the library to develop effective protection programs with goals, objectives, timetables, and benchmarks to counter specific threats such as fire, theft, vandalism and mutilation, and personal safety.

3.5 preparing and keeping current a library fire evacuation plan and an emergency disaster plan for each library with specific staff instructions and directions, including emergency closing and evacuation, staff notification, life safety responsibilities, maintenance of building integrity and utilities, library stand-alone procedures, and emergency conservation and recovery. See Section 4.

3.6 preparing a security operations manual for routine, operational and emergency situations, which is especially useful during the absence of higher level managers. See Section 6.

3.7 ensuring that the person responsible for security/safety needs to follow construction projects to completion to ensure the site is in compliance with safety/security Standards, i.e. American with Disabilities Act requirements; fire alarm systems; swipe cards/lock systems.

3.8 supporting communications between Security Management and Emergency Management agencies.

Section 4. Fire and Emergency Protection

It is suggested that the Library Director, or designee in safety and security matters, should be responsible for:

4.1 integrating a fire and emergency protection program into a library protection policy to avoid and mitigate losses to the library. Fire risk is the major threat to libraries and archives and library protection should be managed accordingly, following the guidance of the National Fire Protection Administration (NFPA) National Standards especially NFPA Standard 909 for the protection of Cultural Resources, Including Museums, Libraries, Places of Worship and NFPA Standard 914 for the protection of Historic Structures, and subsequent revisions. Each state and city may have fire codes additional or slightly different from NFPA standards which can be easily verified with the local fire department. For additional information relating to NFPA Standards refer to the NFPA website: www.nfpa.org. Note that there is a subsequent cost fee to obtain the full context of a particular standard. It should be noted that building codes are primarily intended to protect the safety of the occupants and the fire fighters. Beyond building code minimums there are additional fire suppression and safety systems that can provide both occupant safety and also protect high value Library materials against water damage that will occur from a sprinkler system. Some of these concepts are noted below.

4.2 using reliable early warning fire detection and annunciation systems (visible strobe lights and audible alarm signals) that are both visual in the form of a strobe light and audible by a bell or horn, with signals clear and distinguishable from other signals and easily understood by all users of the library, including persons with disabilities. The systems must comply with NFPA Standards 71 and 72 and its equipment must be approved by Underwriters' Laboratories (UL), Factory Mutual (FM) or similar nationally recognized testing agencies.

4.3 requiring sufficient exits and exiting guidelines, including areas of rescue assistance, following NFPA Standard 101 on life safety. When a building is occupied all exits and exit ways leading to a safe means of egress must be accessible in a manner that does not prohibit the evacuation of the occupants. If doors are equipped with electronic/magnetic devices they must release in a fire evacuation situation or loss of power.

4.4 requiring a fire service physical inspection of the library to plan its tactical response, verify the library’s compliance with local and state fire codes as well as acceptable fire safety standards and review the use of fire prevention practices on all library properties, and review the library's use of fire prevention practices such as control of the use of open flames (by cooking, smoking, candles and welding). A fire service should also inspect electrical appliances before use including the use of timers with heat generating appliances and check

compliance with fire service room occupancy limits. Use of electrical appliances should be limited to a staff room.

4.5 publishing a library evacuation plan and displaying emergency exiting diagrams and instructions for staff and patrons, including persons with disabilities, with a minimum of one fire drill exiting per year, in which the staff fully participate.

4.6 ensuring that fire detection systems are monitored continuously at a separately located station such as the municipal police or fire station and a library monitoring center (whether it be a panel in the occupied building if on its own and/or linked to a security monitored center). Appropriate NFPA Standards such as NFPA Standard 72 should be followed, using equipment that is approved, and is periodically inspected and recertified by UL. If an uncertified monitoring facility must be used because of local necessity it should be done only with the approval of the local security and fire protection authorities, with regular on-site inspections for its adequacy.

4.7 installing fire service approved firefighting equipment of an approved kind and quantity, including portable fire extinguishers visually inspected monthly by library personnel and inspected annually for maintenance purposes and tagged by an approved fire extinguisher maintenance company (NFPA Standard 10) and placed in strategic locations throughout the library, following NFPA Standard 10, and when possible water standpipe and hose systems, following NFPA Standard 14. Staff should receive training in the appropriate use of fire extinguishers.

4.8 setting a high priority on protecting the library with an automatic fire suppression system, since libraries hold combustibles and often have structures with open stairwells. A safe, reliable, and often recommended system for libraries and archives is a cross-zoned, wet-pipe water sprinkler extinguishing system specified for minimum sufficient water release, for installation throughout the library, but especially in areas with special risk such as mechanical rooms, kitchens, shops and work spaces using flammables, chemicals and electrical equipment. Automatic fire suppression systems should follow NFPA Standard 11 on medium and high expansion foam systems; NFPA Standard 12 on carbon dioxide extinguishing systems; NFPA Standard 13 on installation of sprinkler systems; NFPA Standard 17 on dry chemical extinguishing systems; Standard 75, Standard for the protection of information technology equipment; NFPA Standard 2001 on clean agent fire extinguishing systems and NFPA Standard 12 A on Halon 1301 fire extinguishing systems. It should be noted that Halon is now a banned greenhouse gas but a stockpile is available for re-charging existing systems.

4.9 planning an effective physical layout of the library with fire walls and doors and the use of automatic door closures following NFPA Standard 101, Chapter 8 on life safety and fire dampers and fan shutoffs in ducts to prevent the spread of

fire and smoke throughout the library, following NFPA Standard 90A, for air conditioning and ventilating systems, to include an efficient means to ventilate smoke and toxic gases created by fire. Raise awareness with staff and patrons to ensure closure of fire doors to contain a fire situation from spreading.

4.10 requiring regular inspection and testing of fire detection, annunciation, suppression and fire fighting systems following appropriate NFPA standards, local fire service codes and equipment recommendations, whichever is more stringent. These include NFPA Standard 13, Chapter 26 on the inspection, testing and maintenance of sprinkler systems and NFPA Standard 72H on testing protection signaling systems.

Section 5. Physical Barrier and Lock and Key Security

It is suggested that the Library Director, or designee in safety and security matters, should be responsible for:

5.1 integrating a physical barrier and lock and key security and/or card system program into a library protection policy that requires adequate and regular use of physical security closing and locking devices and sound lock and key accountability.

5.2 employing perimeter protection, not leaving external library, non-public, or high value perimeters open or unprotected, nor permitting a contractor to do same. Adequate operable closure hardware for doors, windows, hatches, gates and cabinets, especially locks, should be furnished. The Director should match the relative security of devices and carriers, including balancing the protection afforded indoor openings by the door, door frame, hinges and lock, to the level of security and safety needed.

5.3 preferring physical perimeter barriers to electronic or staff security checks. This includes instructing staff to regularly close unused or unnecessary doors, windows, and other exits. While programmable access control systems with digital keypads or cards or biometric readers are encouraged, these and alarms are not adequate physical security by themselves.

5.4 securing high security perimeters with solid surfaces and high security closures on its openings. High security perimeters are perimeters holding special collection storage and other high value objects and the library perimeter, which includes above and below ground level, the roof, open balconies, and atriums.

5.5 using good quality, pick-resistant deadbolt locks on high security perimeters, which use keys whose blanks are not commonly available from locksmiths without a registered signature. Door, window, or hatch hinges and installation nuts or screws for high security hardware should be secured and located on the protected side of the opening. Key openings on the external side of high security perimeter doors that are not needed for operations should be fused closed in order to deny their use by lock picks and unauthorized keys. Exterior windows should use pins or locks not easily opened by breaking panes of glass without detection, not cam locks as the major device. Sliding glass windows should use double cylinder deadbolt locks, not thumb turn locks. Double doors and double hung windows may require reinforcement with bars, posts and pins.

5.6 requiring exhibit cases to be firmly constructed or fixed to the wall to avoid easy entry. Use of security screws and brackets, hangers with locking devices or other similar methods that require knowledge of the attachment systems and

time to remove them should be used. Cam locks, except high security types, should not be used for display cases.

5.7 requiring an effective key and/or cardkey program as part of the access control program for accountability, control, and strong physical security. This should be planned and operated by one person, preferably security staff or a staff person closely allied with security operations.

5.8 requiring all keys and/or cardkeys to high security areas to be issued, signed for, and returned daily to security where they should be stored in an adequately locked container in the library and accounted for each night.

5.9 accounting for, keeping written record of, and having physical control of keys and/or cardkeys not issued and key blanks. An annual key audit should be conducted to insure that all keys and/or keycards issued and/or not issued are accounted for and if necessary replace keys and/or locks.

5.10 limiting key and/or cardkey abuse by not issuing keys or cardkeys with bit codes or room numbers to be marked on them. Any contracted locksmith should be bonded.

5.11 requiring secure methods of retaining technology based equipment and peripherals.

Section 6. Security Duties and Security Personnel

Not all libraries will require fulltime security personnel. Should a library determine that they do require such service the following are suggestions to help implement a security force. These guidelines do not include all requirements. It is recommended that the organization work with their local law enforcement agencies, and comply with local and state government standards/laws.

It is suggested that the Library Director, or designee in safety and security matters, should be responsible for:

6.1 integrating a security program into the library protection policy for all staff in the library in order to provide security monitoring of conditions. Staff security should include self protection, protection of immediate surroundings and property, and minor additional security duties when there are no full-time security personnel (ex.: clearing the building during fire alarms). Libraries with designated security officers should continue this practice even when the Library Director or security manager employs security officers, referred to here as "security personnel."

6.2 requiring all staff to protect themselves and their immediate property and take action when necessary to protect lives and property and report any difficulties to the appropriate personnel for quick correction. All staff should be required to fulfill basic security duties such as being aware of who is in their work area(s), following routine security procedures for staff and property, reinforcing patron rules of conduct, keeping valuables out of sight if not locked up, completing first-person opening and last-person closing procedures, and following emergency instructions. At no time are staff required to place themselves in personal danger in the performance of these basic security duties.

6.3 providing sufficient security personnel at all times that the building is occupied under the direction of a security manager. Sufficient staffing includes consideration of adequate security coverage during breaks, shift changes, illnesses, and days off, weekends, holidays, and other absences. Additional security personnel may be required when there are significant general or specific threats and risks to persons, collections or the library.

6.4 requiring security personnel to be physically and mentally fit to perform in that capacity detailed in Appendix A as Suggested Security Personnel Qualifications. Complete a background check successfully, described in Appendix B as Staff Pre-Employment Screening Guidelines. Comply with state and local requirements.

6.5 requiring security personnel to be responsible not only for security, but also good customer service to patrons and staff, protection of life and property, fair rule enforcement, completion of all fair orders and instructions, staying on

duty until relieved in the absence of superiors, and the coordination of emergencies of the library.

6.6 providing security personnel with a procedures manual and sufficient training, including post or patrol assignment security responsibilities, the handling of patron and staff problems and complaints, the handling of library and protection equipment, and the handling of violence and emergencies, especially during the absence of high level managers. The minimum training for security personnel should be one day of classroom instruction prior to working and continuing on-the-job training by a competent and experienced instructor or security manager. Security supervisors should be adequately trained. Licensed, armed, and medically qualified security personnel require regular retraining and recertification.

Section 7. Personal Access and Parcel Control

It is suggested that the Library Director, or designee in safety and security matters, should be responsible for:

7.1 integrating a personal access and parcel control program into the library protection policy in order to protect lives and assets at the library. The program should use physical barriers, entry/exit control devices, and security staff checks and should include everyone using the library, including staff of every category, board members, volunteers, contract and construction workers, interns, researchers, maintenance staff and office visitors, without exempting any library user from security controls. The personal access program shall define controlled areas by geography and by time, such as secured areas of high value, continuously; establish the limits and conditions for entry and use, including by time and day of week; and establish a means for staff to gain access to those areas to carry out their duties.

7.2 requiring those staff who have been prepared to perform basic security functions to identify and determine the authority or purpose of persons before permitting persons to cross secured library perimeters. As a minimum, security staff should protect the perimeter for entering and leaving non-public areas and high security areas during open hours.

7.3 requiring security staff to maintain and use security registers to record consistently the entry and departure of visitors to non-public areas and to all areas during non-public hours. Security staff should also use these or similar registers to record the issue and return of visitor badges, after-hours entry and departure for everyone, and the removal of property from the library and grounds. Contractors and construction staff should be required to comply with this system or be segregated from library areas.

7.4 providing its staff a symbol of authorized access with some visible form of identity such as a name plate, emblem, uniform, or badge to reassure patrons of a staff presence and discourage patrons from imitating the work privileges and behaviors of staff. Security staff should issue a one-time entry badge or authorization card for visitors to non-public areas, with requirements to comply with visiting rules and be escorted during visits to high security areas.

7.5 suggest that staff wear a staff photo identification badge or card to permit easy and safe recognition for entry into non-public areas (when the total number of staff exceeds more than can be easily recognized by everyone, such as about thirty people). A good photo identification badge or card system should be no smaller than 2 inches by 3 1/2 includes in size which is laminated or otherwise protected from tampering or forgery and include the name of the library, a reasonable photo, the person's full name (if required), a register number and/or

color identifying the staff function and a date of expiration. A full record of badges or cards, preferably a duplicate of what is issued, should be kept.

7.6 limiting and controlling access to secured areas containing sensitive and high value materials such as areas with special collections, negotiables, and sensitive records. Visitors should be limited by means such as registry, key issue, alarms, and/or security escort entry requirements. Visitors should positively identify themselves, demonstrate a clear need to visit, sign in and out, and be accompanied at all times by security staff or qualified professional staff. Security should require a ratio of one security escort for every ten persons when groups visit.

7.7 limiting and controlling object entry, if desirable and feasible, to prevent dangerous and unwanted objects from entering and exiting, and to prevent illegally or inappropriately obtained materials from leaving. The Library Director should require staff with primary security duties to perform visual and physical inspection of all materials entering and leaving.

7.8 requiring all library materials being removed from the library to be documented at the appropriate checkout desk as a loan. Loans for exhibits will require additional procedures.

7.9 requiring a staff person with primary security duties to review regularly the safety of incoming mail and the security of outgoing mail, including parcels left at the door for pickup or drop off. Unidentified packages left unattended shall be reported to security.

Section 8. Security Alarms and Electronics

There are a variety of security and intrusion alarm systems available that should be explored and potentially integrated into the Library. They range from hardwired systems with protection against power cuts and tampering to battery powered systems. There is also a wide variation in the quality level of all these systems. Because they are electronics they are constantly changing in their capabilities, cost and ability to integrate into other systems in the building. The Library Director should consult with a security system consultant to gain a full understanding of the benefits of various systems as they would relate to the unique configuration and size of the specific Library Building. A reliable security system requires professional selection and application for overall good alarm coverage. Also important are secured communication lines and backup power supply. Once installed and operational, local alarms must be audible. It is essential that staff respond consistently and rapidly. If possible, alarms should be audible in all locations, not just at the point of contact or trouble. This will assure that others not in the area are able to monitor and respond if necessary. Proper adjustments, inspection, testing and maintenance of all alarms are essential.

It is suggested that the Library Director, or designee in safety and security matters, should be responsible for:

8.1 assigning staff to monitor and respond to alarms. When no security staff is available, other library staff must also know how to properly monitor and use the alarm system.

8.2 using security alarms to provide continuous alarm protection where needed. Other areas may just need to be alarmed during certain times. Alarm systems for areas that require high security measures should have overlapping security protection. This could be other types of alarms, cameras, or electronic locks. 24/7 monitoring by a security company or police station is also suggested.

8.3 assuring that every security alarm is responded to with speed and consistency. Every alarm should be both audible and visual. When the library is closed, the Library Director must require that the security manager, a security company, or police officer(s) make a consistent and rapid response to each and every alarm. The person or company responding to alarms must investigate and report on each occurrence the results in a timely manner.

8.4 fully alarming the exterior perimeter of the library building. This includes all openings such as exterior doors, ducts, hatches, and windows that open to the outside. The point of entry will ideally be fitted with a magnetic contact. If the contact is broken, an alarm will alert the monitoring station. The alarm contacts should be installed on the inside or protected side of the opening. Exterior surfaces with glass, including doors, panels, and skylights should use detectors that either sense breaking glass or motion.

8.5 using motion detectors in strategic places throughout the library while the building is closed. The detectors will sense any unauthorized movement after hours. Some sensors should be visible and others should be hidden so that anyone trying to maneuver around the visible sensor is detected.

8.6 carefully selecting alarms for objects and rooms, especially where high value or high risk materials are stored. Special collection storage rooms and walk-in vaults where high value objects are kept should remain continuously locked and alarmed. Tattle-tape and similar radio frequency (RF) field labels should be imbedded in high risk library and archival materials. Safes and vaults which contain high value materials should be located inside areas that remain locked and alarmed at all times.

8.7 using closed circuit television (CCTV) security monitoring systems where appropriate. If a person is appointed to watch a monitor(s), that individual must be very responsible and have a very high and consistent ability to recognize problem situations or conditions that require security attention in real time. However, CCTV is very useful in playback mode and if connected to a digital recorder or downloading to a server. CCTV is an asset when needed to verify event occurrences, especially if crime is involved, but also when just needed to observe readers using high value materials. CCTV used in conjunction with an electronic access control system provides an additional layer of protection.

8.8 integrating and using an electronic controlled access system for limiting and controlling access to secured areas containing sensitive and high value material. Such a system consists of an identification badge (proximity card or fob), a door reader, a control, and a host software application. This system is a solution for controlling access and recording events that occur with or without alarm features or the use of CCTV.

8.9 activating or deactivating alarms at the beginning and end of the day. Staff who open and close facilities should be authorized to also activate or deactivate the same alarms. These individuals and any other staff who may face threats or be subjected to excessive hostility should be protected from harmful situations by using a silent duress/panic alarm. Such an alarm would be hidden under the counter or desk. If a situation occurs, the staff person would only need to discretely press a button to summons help from security, police, or both.

8.10 installing hard wired alarm systems whenever possible. Where this is not practical, wireless systems will work. However, they must be maintained to assure the batteries are fresh and must be tested frequently.

8.11 assuring that the security alarm wiring is protected from tampering. Also important is that the security system is connected to backup system (generator, batteries, or other) in the event of a power failure.

8.12 requiring that the proper adjustments, inspection, testing and maintenance are performed are a routine basis. Poorly adjusted, improperly positioned, uninspected, and untested alarm sensors do not protect.

Section 9. Crime Prevention through Environmental Design (CPTED)

The process of designing security into buildings and grounds is known as Crime Prevention through Environmental Design (CPTED). It involves arranging or designing the built environment to reduce the opportunity for and fear of crime and disorder. This approach to security design recognizes the intended use of the space in a building and is different from and complimentary to traditional security practices, which focus on denying access to a crime target with barrier techniques such as locks, alarms, card access, closed circuit TV, fences, and gates. CPTED takes advantage of opportunities for natural access control, surveillance, and territorial reinforcement. If the design process includes CPTED, it is possible for natural and normal use of the environment to largely meet the security goals and technical protection methods. It is recognized that the best opportunity for incorporating CPTED principals come during time of facility planning or change, but awareness of the ideas can allow the normal ongoing small changes to incorporate these concepts. (1)

It is suggested that the Library Director, or designee in safety and security matters, should be responsible for:

9.1 being aware of the concept of CPTED and when the opportunity arises explore CPTED best practices in the arrangement of windows, entrances, furnishings, lighting, staffing, landscaping, parking and other physical items. The items listed below are examples of issues that should be considered in the arrangement or design of facilities.

9.2 incorporating natural surveillance increase the threat of criminal apprehension by taking steps to increase the perception that people can be seen. Natural surveillance occurs by the placement of physical features, activities and people in such a way as to maximize visibility and foster positive social interaction among legitimate users of private and public space. Potential offenders feel increased scrutiny and limitations on their escape routes.

a. Place windows overlooking sidewalks and parking lots.
b. Leave window shades open and partial interior night security lighting on.
c. Use passing vehicular traffic as a surveillance asset.
d. Create landscape designs that provide surveillance, especially in proximity to designated points of entry and opportunistic points of entry.
e. Use the shortest, least sight-limiting fence appropriate for the situation.
f. Use transparent weather vestibules at building entrances.
g. When creating lighting design, avoid poorly placed lights that create blind-spots for potential observers and miss critical areas. Ensure potential problem areas are well-lit: pathways, stairs, entrances/exits, parking areas, ATMs, phone kiosks, mailboxes, bus stops, storage areas, dumpster and recycling areas, etc.
h. Avoid too-bright security lighting that creates blinding glare and/or deep shadows, hindering the view for potential observers. Eyes adapt to night

lighting and have trouble adjusting to severe lighting disparities. Using lower intensity lights often requires more fixtures.

i. Place lighting along pathways and other pedestrian-use areas at proper heights for lighting the faces of the people in the space (and to identify the faces of potential attackers).
j. Natural surveillance measures can be complemented by mechanical and organizational measures. For example, closed-circuit television (CCTV) cameras can be added in areas where window surveillance is unavailable. It is also suggested that CCTV cameras should also be placed in areas of vulnerable attacks that are not near windows. Selection of the appropriate cameras and lens is important and exterior cameras should be day-night cameras and in extremely darken areas it would be suggested to use cameras equipped with infrared lighting.
k. Use caution when planting shrubbery as not to provide or obstruct the view of customers or staff by providing a opportunity for criminals to hide.

9.3 utilizing natural access controls limits the opportunity for crime by taking steps to clearly differentiate between public space and private space.

a. By selectively placing entrances and exits, fencing, lighting and landscape to limit access or control flow, natural access control occurs.
b. Use a single, clearly identifiable, point of entry.
c. Use structures to divert persons to reception areas
d. Incorporate maze entrances in public restrooms. This avoids the isolation that is produced by an anteroom or double door entry system.
e. Use low, thorny bushes beneath ground level windows.
f. Eliminate design features that provide access to roofs or upper levels.
g. Natural access control is used to complement mechanical and operational access control measures.

9.4 endorsing the idea of territorial reinforcement promote social control through increased definition of space and improved proprietary concern. An environment designed to clearly delineate private space does two things. First, it creates a sense of ownership. Owners have a vested interest and are more likely to challenge intruders or report them to the police. Second, the sense of owned space creates an environment where "strangers" or "intruders" stand out and are more easily identified. By using buildings, fences, pavement, signs, lighting and landscape to express ownership and define public, semi-public and private space, natural territorial reinforcement occurs. Additionally, these objectives can be achieved by assignment of space to designated users in previously unassigned locations.

a. Maintain premises and landscaping such that it communicates an alert and active presence occupying the space.
b. Provide trees in residential areas. Research results indicate that, contrary to traditional views within the law enforcement community, outdoor

residential spaces with more trees are seen as significantly more attractive, safer, and more likely to be used than similar spaces without trees. It should be noted that as spaces are made more attractive for use through the addition of elements such as trees, these same items can become hiding areas and block visibility for cameras. Care needs to be taken to allow these security concepts to work together.

c. Display security system signage at access points.
d. Place amenities such as seating or refreshments in common areas in a commercial or institutional setting helps to attract larger numbers of desired users.
e. Scheduled activities in common areas increases proper use, attracts more people and increases the perception that these areas are controlled.
f. Territorial reinforcement measures make the normal user feel safe and make the potential offender aware of a substantial risk of apprehension or scrutiny.

Footnotes:

1 - Atlas, Randall. *21st Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention*. Boca Raton: CRC Press, 2008. 545p.

Appendix A: Suggested Security Staff Qualifications

It is suggested that the Library Directory should establish reasonable and justifiable qualifications for security officers, here called staff with primary security duties, detailed in Section 6. Security enforcement requires legal consultation and coordination with local law enforcement. Emergency or security staff require medical training and certification if they provide emergency first aid and cardiopulmonary resuscitation. Armed staff require agreement and coordination with local law enforcement, legal offices and protection specialists; compliance with local, state or national licensing laws; and additional employment screening, training, licensing and supervision.

Physical Capabilities	**Qualification Level of Importance**
Able to walk a patrol 8 hours a day	Mandatory
Hold a heavy door to open for minutes at a time	Mandatory
Place a person at least 100 pounds in a wheelchair	Desirable
Climb steep stairs or a ladder	Mandatory
20/20 vision	Desirable
(corrected to 20/40 with glasses)	(Mandatory if armed)
Hear normal conversation (prosthetics are acceptable	Mandatory
Bend, stoop or work with hands above shoulder level	Mandatory
Talk intelligibly over a telephone or portable radio and be understood by other members of the force.	Mandatory
No amputations, deformities or disabilities that would prevent satisfactory performance of duties.	Mandatory
Present a neat, clean, non-threatening appearance	Mandatory
Lift a small child (50 pounds) and carry in a rescue	Mandatory
Mental/Educational Capability	
High school diploma or equivalent	Mandatory
Read and understand written material in English and the language of the security force.	Mandatory
No history or presence of any significant psychiatric disorder	Mandatory
Emotionally stable	Mandatory
Other Capabilities	
No criminal conviction record indicating moral turpitude	Mandatory
No history of violent acts that would indicate the candidate would harm a patron or employee.	Mandatory
No history of child abuse/sexual abuse	Mandatory
Valid driver's license and safe driving record (Mandatory if driving is required)	Desirable
Emergency first aid qualified	Desirable
Cardio pulmonary resuscitation (CPR) qualified	Desirable
Local or state guard license or certificate	Desirable
Pre-employee polygraph where permitted or paper & pencil honesty test.	Desirable
Physical examination by a physician	Desirable
Drug test	Desirable
At least 18 years old	Mandatory

Appendix B: Staff Pre-Employment Screening Guidelines

With the advice of legal counsel, human resources, loss protection professionals and law enforcement officials, it is suggested that the Library Director should manage the conduct of background checks as part of an internal security plan that is integrated into the library protection policy for the protection of staff, workers and patrons. It is suggested that the Library Director should require all library staff applicants and appointees to complete all basic application requests honestly and completely, with final acceptance dependent upon the completion and acceptability of these.

- A written job application that accounts for all periods of employment and gaps between employment during the past five years, to ensure that the applicant not avoid including any incarceration, employment termination or other relevant condition. Note that applicants who submit incomplete or dishonest materials should be given one opportunity to correct their information. Those who misrepresent or avoid questionable information should be subject to further investigation for final acceptance to determine whether this behavior would be likely to continue while employed at the library. A note should be included in any corrected record of the difference between first and second application information. Because prior employers are often reluctant to release negative information, even for legal purposes, a safe, all-encompassing question that deserves a fair answer is whether the previous employer would consider rehiring the applicant.

- A signature to verify that all application materials are correct and personally done, with permission or release form for the library to conduct further background investigation record checks. Note that this should advise applicants that records will be checked and that non-acceptability shall be cause for not hiring.

- An interview in person by a responsible interviewer at the professional level. Note that the interview should double-check that the materials submitted belong to the person being interviewed and were completed by that person. Skilled interviewers should note behaviors that may indicate unusual nervousness, incompleteness or deception about any data or issue that merit further investigation.

- As appropriate, several personal and professional references who vouch for a person's character and integrity. Note that an applicant or appointee may arrange for someone to respond or pose as a reference. References should be checked to determine that they are who they say they are by checking references' organizations with whom they are affiliated, requiring them to receive mail at the addresses listed and cross-checking given telephone numbers in the telephone directory or with directory assistance.

- Educational achievements and licensing data, especially where relevant to the job. License checks show the library's intention to verify work-related skills and work histories. An educational achievement check verifies the library's correctness in awarding a work position based on academic achievements. Note that a driver's

license check should indicate if the applicant has a major health, drug or alcohol abuse problem that interferes with safely operating a vehicle. A guard license or certification check, including union card check, should indicate if the applicant has legitimate work qualifications and a length of satisfactory work in the field.

The Library Director should evaluate each staff position for vulnerability that a person in that position presents to the library, to staff and to patrons, and establish a corresponding level of background check to balance that vulnerability. Examples and suggestions of three category levels are:

- Basic level background check: Designed for staff with little or no access to special collections, patrons, valuables, sensitive information or the management of negotiables. This may include staff who work outside the facility and those who move freely in the office spaces but do not have clear or obvious access to any of the above.

- Intermediate level background check: Designed for staff with typical access to collections and patrons but little or no access to valuables, sensitive information or the management of negotiables. This is "typical" staff access to the library during public and office hours and non staff visitors with a similar capacity. These persons may move through the collection areas unattended before public hours or before offices close, without access to special collection or high security storage. They do not manage special collection materials or valuables, do not have high security keys, do not have after hour access and are not assigned in a regular public contact role that may place a patron or the library in jeopardy. Note that an intermediate level staff check requires more certainty to personal identification and accuracy of records checks, with these additions:

    - A criminal conviction history check for a period of no less than five years prior to the date of application or as far back as is legal in the jurisdiction. Note that a policy check or "name check" requires a check by Social Security Number and that a juvenile criminal record is not able to be released and checked.

    - References from previous places of employment for at least the past five years. Note that a prior employment check reports working difficulties and may uncover legal difficulties that were not reported in the criminal conviction history.

- Advanced level background check: Designed for staff with a level of access that poses a higher potential risk, with regular access to special collections, patrons, valuables, sensitive information or the management of negotiables. This includes staff with primary security duties; mail room, loading dock and shipping and receiving staff; staff with access to sensitive information, especially computer information and computer administrative privileges; cashiers and cash handlers, accounting and purchasing staff; and staff with access to special collection

storage, high security areas and high security keys. Advanced level staff checks shall require a complete application process above, plus:

- A reference from all previous employers in the past ten years and a criminal conviction history check for a period of no less than five years prior to the date of application or as far back as is legal in the jurisdiction. Note the intermediate entry above for criminal conviction checks and the previous employer check note from the basic application check.

- A minimum of three references in addition to those previously provided by the applicant, obtained during an interview with the applicant. Note the entry on references above and that the sooner the check may be conducted after receiving the references during the interview, the more valid it may be.

- A consumer credit check to determine the applicant's credit history. Note that credit and payment histories reveal financial responsibilities and pressures, personal habits, lifestyles and spending habits that reinforce an understanding of the applicant's character and possible motivation or predisposition to theft or embezzlement.

- A civil records check to reveal any unreported civil actions that may reflect on the library. Note that permission is required and that a number of different jurisdictions for places of work and places of residence may require inquiries.

- Verification of the education achievements claimed by the applicant. Note that distinguished staff are given privileged status at the library and are publicly known for their academic standing on the basis of educational achievements that should be verified. While transcripts are relatively easy to obtain, numerous awards and achievements may be more difficult to certify.

- A photograph and fingerprints to certify personal identity. Note that fingerprinting requires the taking of good prints and does not require a fingerprint check at the time of hiring. A photograph from the photo identification card process is sufficient. These records may also permit a staff to be identified or removed from a suspicion list during an investigation.

The Library Director should require that all persons managing background checks and investigations undergo advance background checks known as a "full field" investigation, to be conducted and analyzed by a professional consultant or local police officials, not by staff from an umbrella organization that may have concerns or controls that may affect the data or the outcome. The person or persons conducting these investigations

needs simply to report the result of the investigation against the advanced level acceptance standards above, keeping the information permanently on file. No one involved in the background check process at the library is exempt from it. Board members and persons appointed to positions of public attention connected with the library should also undergo this process for the protection of the library.

The security manager or person responsible for security should gather, review and maintain the required background information in a professional and confidential manner and summarize, report and recommend through the personnel director to the Library Director, most confidentially, a final opinion for each applicant.

The Library Director should make a decision with the security director and personnel director for final acceptance for employment. Those making final acceptability judgments should link discrepancies in background checks with potential vulnerabilities at the library and make judgments within local law and good ethical judgment. The Library Director should depend upon the security manager and personnel manager to advocate the best from their professional positions. Each final acceptance decision, change and exception to final acceptability rules or criteria should not be a unilateral decision nor should it have to be unanimous.

Note that this appendix does not define how to determine final acceptability for particular library positions, except for those who review background checks, who must be above reproach. There is no clear-cut criterion for being denied final acceptance except based on civil, legal, and ethical opinions. The background history of the individual should not be the sole criteria for denying employment or promotion, but should be a major factor.

As examples only: applicants with felony records within the recent past, especially for any form of theft and individuals with arrests for use of illegal drugs or narcotics, should be considered subject to denial of final acceptance for intermediate and advanced level access when they have access to high value records and information. Applicants with a record of serious sexual and child abuse convictions should be considered subject to denial of final acceptance for intermediate and advanced level access when they may work closely with patrons and staff. Applicants with older records of criminal or civil convictions or bad credit history may indicate potential risk but not necessarily dishonesty; the security manager may wish to consider the possibility of the applicant to reform.

Library staff who manage and process background information should refrain from gathering and should refuse to record, report or store information that is irrelevant or immaterial to deciding the final acceptability of the applicant, such as material that is legally discriminatory as well as court records for civil disobedience involving moral turpitude, sexual preference or similarly irrelevant data. Legal counsel should determine what information may ever be released to individual applicants or others under the Freedom of Information Act.

Exemptions from undergoing background checks and requiring a positive final acceptance are strongly discouraged but inevitably necessary when information and records are incomplete and decisions must be made. No staff should be exempt from the appropriate, pre-determined level of background check nor any decision postponed for an inordinate length of time. No staff should be exempt from preparing an application or providing a release to authorize a background check. Library managers should avoid exempting persons with high status who may present serious vulnerability to the library, including well known scholars, management and board members and those with high public and professional reputation or standing.

When certain records and information are unavailable to investigators, they may gather and use as optional information:

- A personality profile test, where legal, that is professionally recognized, to determine an applicant's attitude toward honesty, drug use and similar matters.

- A physical examination with drug tests, where legal and properly administered, to determine the applicant's freedom from drug or alcohol abuse.

- A worker's compensation check, where legal, to identify applicants who have left previous posts after committing insurance fraud.

- Checking the candidate’s credit report and motor vehicle state driver’s license could also be considered.

Applications and background check information, as personal information, should be protected in use and in storage, with limited access under high security. Consult with a legal counsel if the applicant or others may legally request its release and under what conditions under the Freedom of Information Act. When practical, applicant files should be sealed in an envelope within the file so that they are available for future reference, but not readily available to those in a personnel management or administrative capacity without a need to know. Application and background check information may be retired to another place of record, under the same high security controls, but never destroyed.