

Table of Contents

1 Safety and Security of Patrons and Staff	4
1.1 Code of Conduct	4
1.2 Incident/Accident Report	4
1.3 Contact Information/Phone Tree	4
1.4 Blood-borne Pathogen Training	4
1.5 Hazardous Materials Training	4
1.6 Background Checks	5
1.7 Identification Checks	5
1.7.a Patrons in non-public areas	5
1.8 Workplace Violence Policy	5
1.9 Staff/Patron Health and Welfare	5
1.9.a Overuse/repetitive motion injuries	5
1.9.b Harassment, threatening behavior, assault, and stalking	6
1.9.c Sexual harassment	6
1.9.d Threatening Behavior	7
1.9.e Stalking	7
1.10 Major emergencies/incidents	8
1.10.a Natural	8
1.10.a.i Fire	8
1.10.a.ii Flood	8
1.10.a.iii Tornado/Hurricane	8
1.10.a.iv Earthquake	8
1.10.b Man-made	8
1.10.b.i Bomb threat	8
1.10.b.ii Armed intruder	8
1.11 Minor emergencies/incidents	8
1.11.a Disruptive behavior	8
1.11.b Suspicious Behavior	8
1.11.c Theft of library property at a theft detection system	9
1.11.d Theft of library property, personal property, vandalism	9
1.11.e Sexual misconduct	10
1.11.f Alcohol/drug problems	10
1.11.f.i Persons under the influence	10
1.11.f.ii Drugs - witnessing sale or use	11
1.11.g Accidents/injuries/illness	11
1.11.h Children (Lost)	11
1.11.i Children (Missing)	12
1.11.j Suspected Child Watchers	12
1.12 Privacy	13

2 Safety and Security of Building and General Collection	13
2.1 General Procedures	13
2.1.a Alarms/Closed Circuit Video Monitoring	13
2.1.b Security guard/door guard/extra staff	13
2.1.c Locks and keying	14
2.1.d Floor plan	14
2.1.e Closed stacks/restricted access/reserves	14
2.2 Exterior Survey	14
2.2.a Landscaping	14
2.2.b Lighting	14
2.2.c Walkways and Ramps	15
2.2.d Book returns (placement)	15
2.2.e Parking facilities	15
2.2.e.i Parking	15
2.2.e.ii Keys locked in car	16
2.2.e.iii Automobile accidents	16
2.3 Interior	16
2.3.a Building Access	16
2.3.a.i Public Entrances/Exits	16
2.3.a.ii Emergency Exits	17
2.3.a.iii Loading Docks	17
2.3.b Windows	17
2.3.c Interior lighting	17
2.3.d Stairways	17
2.3.e Elevators	18
2.3.f Restroom security	18
2.3.g Signage	18
2.3.h Circulation Desks & Checkout Machines	18
2.3.i Property marking	18
2.3.j Money handling	19
2.3.k Meeting/Group Study Rooms	19
2.4 Fire prevention	19
2.5 Power Failure	19
2.6 Gas Leak	20
2.7 Explosions	20
2.8 Water Emergencies/Damage	20
3 Safety and Security of Special Collections	20
3.1 Survey	21
3.2 Key/Key Card Security	21
3.3 Lockers	21

3.4 User Registration	22
3.5 Reading Room Practices and Policies	22
3.6 Inspection of Materials Before and After Patron Usage	22
3.7 Identifying or Marking Collection Materials	23
3.8 Disaster Response for Special Collections	23
4 Safety and Security of Electronic Files and Systems	24
4.1 Know who to call	24
4.2 Keep training current	24
4.3 Hardware and peripherals	24
4.4 Label all hardware and peripherals	25
4.5 Use surge protectors	25
4.6 Password protection	25
4.7 Acceptable internet use policies	25
4.8 Access settings	26
4.9 Filtering	27
4.10 Virus, Spyware, Malware	27
4.11 Firewalls and partitions	27
4.12 Encryption	27
4.13 Electronic and paper waste	28
4.14 Backup	28
4.15 Share security breaches and solutions with other institutions	28
References	29
Appendices	31

1. Safety and Security of Patrons and Staff

Safety and security of our patrons and staff is of the utmost priority for our library. Any staff member is authorized to take action in the event that the safety and/or security of another staff member or patron appears threatened. Management will support the staff member's actions. However, please strive to keep all interactions with patrons and other staff professional and polite. Bring in other staff members to assist you if necessary. Document everything and practice being an "expert witness." If the situation is beyond your level of training, please contact the person in charge. Use the following guidelines to help determine how to handle certain situations.

1.1 Code of Conduct (SEE DIFFICULT PATRONS CHAPTER OR ETHICS AND STANDARDS OF CONDUCT CHAPTER)

1.2 Incident/Accident Report (SEE DIFFICULT PATRONS CHAPTER OR APPENDIX B)

1.3 Contact Information/ Phone Tree

Create a document with important contact numbers.(SEE PReP template <http://westpas.org/workshop-docs/>)

1.4 Blood-borne Pathogen Training

All employees should be trained in handling and exposure to blood-borne pathogens. This training should comply with OSHA Standards (SEE OSHA WEBSITE <https://www.osha.gov>). Documentation that annual training has been completed will be retained in the employee records. If you have not received this training or feel your training is out of date, please notify the person in charge and human resources (SEE HUMAN RESOURCES CHAPTER)

1.5 Hazardous Materials Training

All employees should be trained in safe handling and storage of hazardous materials that are commonly found in the library. This training should comply with OSHA Hazard Communication Standards (SEE OSHA WEBSITE). Documentation that annual training has been completed will be retained in the employee records. If you have not received this training or feel your training is out of date, please notify the person in charge and human resources (SEE HUMAN RESOURCES CHAPTER).

1.6 Background Checks

All staff members, student workers, interns, and volunteers must submit to a background check prior to their employment at the library. The more access an individual's position entails, the more rigorous the background check will be.

1.7 Identification Badges

While on duty in the library, staff and volunteers will wear badges so that patrons can find you and so that unauthorized persons can be quickly identified

1.7.a Patrons in non-public areas

Patrons are not permitted in staff areas or in restricted areas (e.g. special collections) without supervision. All staff have a responsibility to speak to someone in these areas that they do not recognize.

PROCEDURE: If an unfamiliar person is seen in a staff area of the library, offer to escort the person to the appropriate office or nearest public area. The person may not be aware that he or she is in a non-public area, or he/she may have been directed to an office for a specific reason. Be professional and courteous. If the customer refuses to leave the area, call the person in charge or security. Fill out an incident report.

WHAT TO SAY: Excuse me, may I help you find something? This is a staff area of the library. Let me take you back to the public area.

1.8 Workplace Violence Policy

Report any suspicions or observations of workplace violence to the person in charge. Staff will conduct annual workplace violence training. Current certifications of this training will be kept in the individual's personnel file. An example of workplace violence training can be found at <http://media.cpms.osd.mil/faslerd/employee/menu.htm> (SEE HUMAN RESOURCES CHAPTER)

1.9 Staff/Patron Health and Welfare

1.9.a Overuse/repetitive motion injuries

It is the library's policy to avoid/minimize any repeated or overuse injuries/problems to patrons and/or staff by providing the following equipment and best practices: ergonomic equipment and furniture, glare reducing screens, keyboards, scheduled breaks for staff,

having staff rotate tasks to avoid repetitive use injuries. If a staff member feels that they need additional accommodations, please contact the person in charge. If a staff member is seeking compensation for work related injuries, please contact Human Resources. (SEE HUMAN RESOURCES CHAPTER)

1.9.b Harassment, threatening behavior, assault, and stalking

If a patron or staff member is subjected to harassment, threatening behavior, assault, or stalking, follow the procedures below. If the behaviors continue, contact police and (for staff against staff incidents) the person in charge and the human resources department (SEE HUMAN RESOURCES CHAPTER). In order to minimize and better manage these situations, two staff people should be scheduled in the building at all times. No staff member should be in the building by themselves.

1.9.c Sexual harassment

Unwelcome sexual advances; requests for sexual favors; and all other verbal or physical conduct of a sexual or otherwise offensive nature are not tolerated by this library. Specific examples include:

Verbal

- sexual innuendoes, suggestive comments, insults, humor and jokes about sex, anatomy or gender specific traits
- sexual comments
- threats
- repeated requests for dates
- statements of a sexual nature about other employees or customers

Nonverbal:

- suggestive or insulting sounds (whistling, catcalls, smacking, or kissing noises)
- sexually suggestive bodily gestures, leering, or obscene gestures
- visual displays such as posters, signs, or slogans of a sexual nature

Physical:

- touching, unwelcome hugging, or kissing
- pinching
- brushing the body
- coerced sexual intercourse
- actual assault

PROCEDURE: Confront patrons/staff observed engaging in activities that can be construed as sexual harassment in the library or on library property. Tell patron/staff to stop the problem behavior. If the patron/staff disregards your warning, ask them to

leave. If they do not leave, call the police. Write up an incident report. In the case of staff against staff harassment, contact the person in charge and human resources. WHAT TO SAY: Your behavior (or language) is considered sexual harassment. Please do not continue (insert inappropriate behavior here). If you continue this behavior you will be asked to leave the library and we will file a police report.

1.9.d Threatening Behavior

Threatening behavior is any action or speech which threatens, has the effect of threatening or intimidating someone, or seems to invade one's personal space. This behavior does not have to be tolerated. Patrons and staff have the right to express anger but not to be abusive to others.

Examples of threatening behavior are:

- Patron following a staff member around the library
- While discussing a problem, a patron begins to yell and invade one's space
- "I'm going to torch the library."

PROCEDURE: Do not argue with a threatening person. Identify yourself as a library staff member. Remain calm and keep your voice low and firm. Attempt to defuse the situation before it becomes physically abusive. Do not put yourself or other staff in danger. Get the assistance of another staff person, if possible. Move the discussion to another more private place. With your colleague, review the situation with customer. Advise him/her that the police will be called if the abuse does not stop. Depending on the situation, it may be advisable to call 911. Notify the person in charge and complete an Incident Report Form

1.9.e Stalking

The law defines stalking as transmitting threats of immediate or future bodily harm, sexual assault, confinement, or restraint or placing a person in reasonable apprehension of receiving threats of immediate or future bodily harm, sexual assault, confinement, or restraint. Stalking behavior should not be tolerated by either patrons or staff. Incidents occurring in the library will be reported to the police.

PROCEDURE: If a staff member is being followed, they should report it to the person in charge. If a staff member notices stalking behavior towards a patron, they should talk to the victim and see if he/she needs help. Try to talk to the stalker. If talking to the stalker does not change their behavior, then ask them to leave and/or call the police. Staff should offer to walk with the victim when they leave the building or be willing to call someone if the customer feels the need to have another person with them. Fill out an Incident Report Form and inform the person in charge.

1.10 Major emergencies/incidents

1.10.a Natural

1.10.a.i Fire (SEE EMERGENCY PROCEDURES CHAPTER)

1.10.a.ii Flood (SEE TO EMERGENCY PROCEDURES CHAPTER)

1.10.a.iii Tornado/Hurricane (SEE EMERGENCY PROCEDURES CHAPTER)

1.10.a.iv Earthquake (SEE EMERGENCY PROCEDURES CHAPTER)

1.10.b Man-made

1.10.b.i Bomb threat (SEE EMERGENCY PROCEDURES CHAPTER)

1.10.b.ii Armed intruder

Weapons (except for those worn by law enforcement) may not be allowed in the library or on the library grounds (check your state laws). Weapons include any kind or size of firearm, knives, switchblades, or other objects held in a threatening manner.

PROCEDURE (NON THREATENING PATRON): If the person with the weapon does not seem agitated or confrontational, first notify other staff and the person in charge. Then approach the person, explain the no weapon policy, and ask them politely to leave. Do not provoke a confrontation. Fill out an incident report form.

WHAT TO SAY (if patron is non-threatening): Hello, my name is _____ and I work for the library. Weapons are prohibiting in the library. Please leave. You may return when you are not carrying a weapon.

PROCEDURE (THREATENING PATRON): If you see a weapon in someone's hand or on their person and feel threatened, call 911. Protect staff and patrons behind desks, tables, etc. Surrender money or property on demand. If possible, alert staff members in other areas of the building and instruct them to keep patrons and staff away from the area where the person is. Alert the person in charge and fill out an incident report.

1.11 Minor emergencies/incidents

1.11.a Disruptive behavior (SEE DEALING WITH DIFFICULT PATRONS CHAPTER)

1.11.b Suspicious Behavior

POLICY: If you observe behavior that is suspicious but you cannot link that behavior to a specific rule or policy, you should still document what you witness. The documentation may be important in creating a “paper trail” should a more significant problem arise in the future. Fill out an incident report, writing down as much detail as possible. If possible, list names, physical features, and addresses of person(s) involved. If appropriate, contact the person in charge, security, and/or the police.

1.11.c Theft of library property at a theft detection system

Security systems are put in place to protect library property. There may be false alarms, unintentional removal of library materials or staff errors that may cause an alarm. When an alarm is activated, search for the cause in a courteous manner and as privately as possible. If the incident does turn out to be a matter of theft, the theft will be handled as outlined in the “Theft of library property” policy (SEE SECTION 1.11.c).

PROCEDURE: When the alarm sounds, ask the person who set off the alarm to step to a private place. Explain that you need to check why the alarm was activated. If no cause can be determined or if it was a false alarm, the staff member should apologize but restate that having the detection system helps protect library materials. If it is determined that there has been a theft, follow that steps outlined in section 1.11.c.

WHAT TO SAY: My name is _____, and I work at the library. Our security system alarm activated. Could you please step over here so we can find out why?

1.11.d Theft of library property, personal property, vandalism

Taking material or property owned by the library without properly checking it out is theft, and is against the law. Vandalizing library property is also against the law.

Examples of theft include, but are not limited to the following:

- Knowingly taking materials out of the library without authority to do so
- Knowingly hiding library material on the body or among belongings with the intent to remove that material
- Using a stolen or fake library card
- Failing to return checked out library materials
- Leaving the library materials not intended for circulation (e.g. rare documents, local history/genealogy, special collections or equipment)

Examples of vandalism include, but are not limited to the following:

- Deliberately cutting, tearing, marking, spitting, or putting other body fluids onto library materials, equipment, or furniture
- Defacing walls or signs
- Damaging restrooms and elevators
- Breaking windows

- Maliciously tampering with any computer system, program, or data

PROCEDURE: Report all incidents of theft or vandalism to the police. Fill out an incident report and notify the person in charge.

WHAT TO SAY: My name is _____, and I work at the library. (Insert action/behavior here) is against the law, and I need you to stop. My supervisor will be here shortly and we will notify the police.

1.11.e Sexual misconduct

Inappropriate public displays of affection are not allowed in the library. Personal contact of a nonsexual nature is acceptable. The following behaviors are not acceptable:

- prolonged kissing
- prolonged hugging
- sitting on another's lap
- engaging in affection of a sexual nature
- Petting
- engaging in sexual intercourse (actual or simulated)
- touching of the genitals

PROCEDURE: If patrons are violating this policy, explain the rule and firmly request that they stop. Follow up and repeat again if necessary. On the third warning, insist that the customers leave the library for the day. Fill out an Incident report and notify the person in charge.

WHAT TO SAY: My name is _____, and I work at the library. We have a policy about public displays of affection. Your behavior is not appropriate in the library. We would appreciate if you followed the policy or we will have to ask you to leave. Thank you.

1.11.f Alcohol/drug problems

1.11.f.i Persons under the influence

Individuals under the influence of illegal drugs or alcohol, or who possess or consume illegal drugs or alcohol in the library or on library property will be asked to leave.

PROCEDURE: If there is a reasonable likelihood that the patron is under the influence of drugs or alcohol, politely ask him to leave for the rest of the day. Explain the policy. Fill out an incident report and notify the person in charge. If the individual is uncooperative or is not capable of following your directions, call 911. If an overdose is suspected, also call 911 for medical assistance.

WHAT TO SAY: My name is _____, and I work at the library. Alcohol/drug use is not permitted in the library or on library property. I will have to ask you to leave today. You can come back when you are not using. OR Have you been drinking today, sir? You appear to be under the influence of either alcohol or drugs and I will have to ask you to leave the library for the rest of the day.

1.11.f.ii Drugs - witnessing sale or use

The sale or use of illegal drugs in the library or on library property is against the law. If you see a drug sale or witness drug use, call the police immediately.

PROCEDURE: Call 911. Give a detailed description of the events and people involved. Keep other patrons safe. People on drugs and/or being arrested can be unpredictable and violent. Do not block the exits. File an incident report and notify the person in charge.

1.11.g Accidents/injuries/illness

Patrons or staff may become ill or injured in the library. When treating any accident/injury/illness always remember to remain calm. Use protective personal equipment and fill out an accident/injury/illness report form. Know the location of first aid kits and AEDs (if your library has them). Follow these procedures:

PROCEDURE: If immediate assistance is needed, call 911. Do not drive the patron/staff anywhere for medical assistance. Do not move the person but try to make him/her comfortable. Stay with the person and reassure them that help is coming. Provide medical aid (CPR, etc.) if you have been trained to do so. Wear personal protective equipment (PPE) to provide first aid. Be careful if body fluids (e.g. blood, urine, saliva) are present. If a Band-Aid needs to be used, give it to the individual and have him place it on the injury himself. Parent may assist their children. Clear the area of bystanders. Recruit other staff members to help if needed. Send someone out to meet emergency services. Fill out an accident report (SEE APPENDIX B) and notify person in charge.

If you have been exposed to blood-borne pathogens, please contact the person in charge and contact the human resources department.

1.11.h Children (Lost)

PROCEDURE: Keep the child close to you or another staff member. Try to locate the parent with the announcement system or by having another staff member look for

parent. Ask the child if he/she has a telephone number of a parent or guardian. If he/she does, call and request that someone pick up the child. If no one is available to pick up the child and it is close to closing time, call the police and explain that there is an unattended child and that the library is closing. File an incident report and notify person in charge

1.11.i Children (Missing)

The responsibility for the care, safety, and behavior of children lies with the parent/guardian, both in the library and on library grounds. A child under age _____ should be accompanied and in the vicinity of a parent/guardian at all times. A child age _____ can use the facilities without immediate supervision, but the parent or caregiver of the child must be somewhere in the building. Children above the age of _____ can use library services without adult supervision.

PROCEDURE: If a parent/caregiver reports a child missing, staff will get a full description of child, including photo if possible. Ask parent/caregiver how extensively they have searched. Check the children's area thoroughly, including bathrooms and offices. Request assistance from other library staff to search their areas. Check outside the library. Call police if unable to locate child. Fill out an incident report form and notify person in charge.

1.11.j Suspected Child Watchers

Adults are not allowed in the children's area unless they are accompanying a child or they are researching children's literature. Adults may not stare at or follow children in the library.

PROCEDURE: Approach the customer. Tell them that it is inappropriate for them to be observing children in the library. Ask them to leave. If they refuse to leave, call the police. Fill out an incident report and notify the person in charge.

WHAT TO SAY (TO 911): This is _____. I work at _____ library. There is a man/woman near our children's area who is staring at the children which is against library policy. I believe that he/she may approach a child here. We need you to intervene. The address here is _____. **(TO THE WATCHER):** My name is _____, and I work at the library. It is inappropriate for you to be watching children in the library. The children's department is for children and their parents or assigned guardians. I must ask you to leave the children's area immediately.

1.12 Privacy

2 Safety and Security of Building and General Collection

2.1 General Procedures

Familiarize yourself with the building. Learn the floor plan and location of exits, controls, electrical boxes, security system, water lines, fire extinguishers, first aid kits, etc. Make sure the building is in compliance with all American Disabilities Act (ADA) requirements (SEE ADA WEBSITE). If it is your duty to perform periodic safety/security checks, note any problems on the security checklist (SEE APPENDIX D) and notify the person in charge.

2.1.a Alarms/Closed Circuit Video Monitoring

If the library has not already done so, consider installing a security system to protect building and collection especially in special collections area. If the library already has a security system, make sure you run periodic checks to make sure that it is working properly. Take note of where all alarms are located and what types they are. The security team should be knowledgeable about what each alarm indicates. Make sure that activating building alarms is part of normal closing procedures.

Alarms should be heard and seen throughout the entire floor including staff, closed stacks and storage areas. Some alarms should flash or strobe to alert the hearing impaired per ADA code requirements

CCTV should cover loading areas, parking areas, stacks, special collections, staff areas and public areas. Video footage should be kept for a minimum of 30 days in case of any incidents. Security should monitor footage constantly and note any suspicious behavior. Cameras should have adequate lighting so that footage will be clear and unquestionable. Cameras near emergency exits can be motion activated.

2.1.b Security guard/door guard/extra staff

Your building may employ a security guard/door guard/extra staff. Be clear about what their duties are and under which situations staff should notify them.

2.1.c Locks and keying

Carry only the keys that have been issued you. Do not share your keys with other staff. Do not share your keys with patrons. Follow the library policy for issuing and returning keys. If you find keys that have not been issued to you, collect them and turn them over to the person in charge.

2.1.d Floor plan

A good floor plan is key in having a safe library (SEE APPENDIX A). Note locations of windows, doors, exits, emergency exits, loading docks, stairways, elevators, emergency equipment, departments, meeting/study rooms, etc. Configure staff work stations and positions to minimize areas that are cut off from staff line of vision. If there are areas not visible from circulation or reference, there should be mirrors placed so that staff can see into the stacks. Patrol less visible areas regularly (or have motion activated CCTV cameras set up).

2.1.e Closed stacks/restricted access/reserves

Limit access to valuable or special collections (SEE SECTION 3)

2.2 Exterior Survey

Exterior security is the first line of defense for collections, staff and patrons, but it is also the most vulnerable. Periodically conduct a safety and security survey of building.

Things to look for when surveying the exterior:

2.2.a Landscaping

- Keep any bushes, hedges or trees trimmed so that they don't block windows, doors or stairwells (they can obstruct the view in and/or out)
- Landscaping can also become home to pests that can potentially cause problems for the library such as insects and small rodents
- Make sure climbing plants are prevented from growing up walls
- Prune branches of trees growing near the building.

2.2.b Lighting

Lights illuminating the parking lot, loading docks, exits, walls, and approaches to the building should be on all the time after dark so that patrons and staff can find their way

safely. Exterior lights should reveal movement/activity outside the building and help security see if anyone is loitering outside or spot suspicious acts. Note any problems on the security checklist and report to person in charge.

2.2.c Walkways and Ramps

Ramps and walkways should be maintained to keep them safe for handicap accessibility. Curbs and curb cuts (these allow for passage of wheelchairs, bikes, etc.) should have some kind of traction. If there is a storm drain under a curb or curbs keep them clear from debris to prevent flooding. Note any problems on the security checklist and report to person in charge.

2.2.d Book returns (placement)

Book returns should not be attached to building, if possible. If your building has an attached book return they should be locked at times when the building is open.

2.2.e Parking facilities

Security cameras should be used to monitor the parking area as well as other exterior parts of the building (SEE SECTION 2.1.a).

2.2.e.i Parking

Patrons/staff must park in designated parking spaces in the library parking lot (if available). Cars blocking drivers or cars abandoned in the library lot may be towed at the owner's expense. A car is considered abandoned if it has been ticketed at an expired meter and/or left in the parking space for over ___ hours. Patrolling the parking lot should be part of the periodic security checklist. If someone feels that someone is following them in the parking lot, see Threatening Behavior or Stalking sections 1.9.d or 1.9.e.

PROCEDURE: Check with patrons/staff in the building to see if the car belongs to one of them. If it does belong to someone in the building, ask the owner to move his or her car. If you cannot identify the owner, call the non-emergency police number to have the car towed. Fill out an incident report

WHAT TO SAY: If the owner of the car towed comes into the library to check on their car: Your car was towed from the library parking lot because _____. You will have to check with the police department in order to reclaim your car. Here is the non-emergency police number _____.

2.2.e.ii Keys locked in car

PROCEDURE: Give the patron a prepared list of locksmiths or assist them in finding a locksmith with a ready reference phone book or online phone directory. Assist them in making a phone call to a locksmith. Note: Most police departments will not respond to calls to open locked cars. They request that you call a locksmith. Fill out an incident report and notify the person in charge.

WHAT TO SAY: My name is _____, and I work at the library. I can help you find a locksmith to get you into your car. Here is a list of locksmiths who are willing to come to the library to assist you. Let me know if you need to use our phone to make a call.

2.2.e.iii Automobile accidents

Report all automobile accidents occurring on library property to the police. Administer first aid, if needed.

PROCEDURE: Check to see if anyone needs medical assistance. If someone is hurt in the, call for medical help. If the injury is serious call 911 (SEE SECTION 1.11.f). Call 911 to report the accident. Ask all of the persons involved in the accident to remain near their cars until the police respond. Fill out an incident report form and notify the person in charge. Make sure to write down the license plates of the vehicles and the names of the people involved.

WHAT TO SAY: My name is _____, and I work at the library. Was anyone hurt in the accident? (If yes) OK, I will call 911. I also need to call the police. It is our policy to notify the police if an accident takes place on library property. Please stay here until the police respond to my call.

2.3 Interior

Interior safety focuses on conditions within the library building itself. Here are things to look for when doing a survey of the interior:

2.3.a Building Access

2.3.a.i Public Entrances/Exits

Ideally, there should be only one entrance/exit for public use. All entrances and exits should have an alarm or be monitored by security staff. If exit door is located in a different place, there should be no way to reenter the building through the exit doors.

2.3.a.ii Emergency Exits

- Nothing should be blocking the doors on both sides
- Signage should be highly visible (lighted signs, large wording, etc.)
- Emergency lights should be equipped with battery backup
- Coordinate tests of door alarms with security
- Should have a push bar that opens from the inside and locks upon exiting the building, with key access from the outside

Note any problems on the security checklist (SEE APPENDIX D) and notify the person in charge.

2.3.a.iii Loading Docks

Doors should be locked at all times, except when there is a delivery

2.3.b Windows

Windows should be locked at all times and be equipped with alarms. Broken windows should be replaced/fixed as soon as possible (SEE WORK ORDER FORM IN FACILITIES CHAPTER).

2.3.c Interior lighting

Lights in certain low use areas may be set to turn on when motion is detected. Emergency lights should be on the generator or battery backup. Test emergency lighting periodically. Note any problems on the security checklist (SEE APPENDIX D) and notify the person in charge.

2.3.d Stairways

- Make sure all stairwells are well maintained and clean of debris
- Make sure traction strips/ridges are intact to prevent slipping
- Make sure handrails are present and secure
- Make sure all fire escape stairwells are in proper working order

2.3.e Elevators

Inspect elevators regularly. Make sure that their certification is up to date. In the event of elevator failure, use the following procedure:

PROCEDURE: In the event of an elevator failure, reassure any persons trapped inside that help is on the way. Call 911 and facilities staff (SEE PReP template <http://westpas.org/workshop-docs/>). The elevator telephone may all be used to summon emergency assistance. If the elevator is stopped at or nearly at floor level, the doors may possibly be opened by gently pushing them apart. If they do not open easily, do not use excessive force. Continue to reassure the patron. Fill out an incident report and notify the person in charge.

WHAT TO SAY: My name is _____, and I work at the library. We know that the elevator is stuck and we have called for help. Help is on the way.

2.3.f Restroom security

Your responsibility to monitor bathrooms will depend on custodian and security staffing schedules. At certain times, you will need to check the restrooms for cleanliness, theft, vandalism, and/or sexual misconduct. Refer to the sections on theft, vandalism, and sexual misconduct if any of these events have occurred. Fill out an incident report and notify the person in charge, custodians, and/or facilities of any problems.

2.3.g Signage

Make sure signage is visible and compliant with ADA guidelines. (SEE FACILITIES CHAPTER, APPENDIX D, AND ADA GUIDELINES).

2.3.h Circulation Desks & Checkout Machines

Position circulation desks near the main exit and/or entrance, especially if there is no security staff. Make sure all patrons with materials have checked them out properly. If you notice someone has walked towards the exit without checking their material, follow instruction in section 1.11.b)

2.3.i Property marking

Use Tattle tapes and targets in combination with security gates.

Another option is the use of RFID (radio frequency identification) technology, a radio transmitter that can be programmed with all types of information. It also permits the storage, retrieval and transmittance of data remotely. For more information, see the American Library Association's website for their guidelines on RFID use in libraries.

Property markings can be added to materials as an additional preventative measure in the form of stamps, etching or bookplates. Property markings make it possible for buyers to contact or notify the library if their materials pop up in a transaction and don't seem like they were properly withdrawn from the collection.

2.3.j Money handling

NEVER count money in the view of patrons. Make sure all money drawers and/or cash registers remain locked when no one is at the circulation desk. DO NOT have a key at the front desk clearly marked that it is for the register/drawer. It should be just like any other staff key. Only certain staff members should have keys and these keys should remain with them at all times.

Do not carry a bank bag in plain sight especially if it has the name of the bank on it and don't always go to the bank at the same time. If possible, arrange scheduled bank pickups so that staff does not have to transport money.

If the library stores money it should be kept in a locked box, in a restricted area or in a safe at all times.

2.3.k Meeting/Group Study Rooms

There should be at least one staff member present when meeting rooms are in use and/or have a security camera installed in or near the room. Any AV equipment should be properly secured.

2.4 Fire prevention

SEE EMERGENCY PROCEDURES CHAPTER

2.5 Power Failure

In the event of a power failure, notify the person in charge, facilities staff, the police and the electric company (SEE PReP template <http://westpas.org/workshop-docs/>). Use backup generators and/or emergency lighting if possible. It may be necessary to evacuate the building. Patrons may not be aware of a problem, especially if there is sufficient sunlight to read by. If the building is evacuated, follow the general instructions for building evacuations (SEE EMERGENCY PROCEDURES CHAPTER). Fill out an incident report. The decision to close the building and/or dismiss staff will be made by the person in charge.

2.6 Gas Leak

In the event of a severe gas odor, evacuate the building immediately (SEE EMERGENCY PROCEDURES CHAPTER). Once outside, notify the person in charge, facilities staff, the police and the gas company (SEE PReP template <http://westpas.org/workshop-docs/>). Fill out an incident report. The decision to close the building and/or dismiss staff will be made by the person in charge.

2.7 Explosions

Explosions may occur as the result of gas leaks or major electrical problems in circuit panels or exterior transformers belonging to the power company. Evacuate the building (SEE EMERGENCY PROCEDURES CHAPTER) and notify the person in charge, facilities staff, the police and the electric company (SEE PReP template <http://westpas.org/workshop-docs/>). Fill out an incident report. The decision to close the building and/or dismiss staff will be made by the person in charge.

2.8 Water Emergencies/Damage

SEE EMERGENCY PROCEDURES CHAPTER

3 Safety and Security of Special Collections

Special collections are unique and exciting as they hold various types of formats and materials including, but are not limited to, archival records, books, audiovisual materials, government documents, maps and photographs as well as the equipment needed to view or hear these materials. It is due to the variety of materials and formats that special collections security and safety is so difficult. They need to be kept safe from the general public and staff as well. A majority of thefts in special collections are committed by staff members, making security of special collections difficult. Items in special collections are valuable and at risk because they are wanted by others. This section addresses best practices for keeping special collections safe for future generations while also allowing access for the current generation. If possible, the library should have a special collections staff member whose sole focus is safety and security and work closely with library security staff.

3.1 Survey

Surveys of special collections areas should be done in a similar manner to other collections and buildings (SEE SECTION 2). During the survey, note these unique features of your special collections area:

- The stacks area should be locked and accessible by special collections staff members only.
- Staff members should monitor all entrances and exits.
- No member of the public should be allowed in the closed stacks without permission/supervision.
- Motion sensors and alarms should be active at all times and powered by an emergency backup generator.

3.2 Key/Key Card Security

Staff access to all nonpublic areas should be controlled with usage of keys, key cards or keypads/codes. Key card systems should be able to limit and track access to specific areas and keep a detailed log of the date, time and location key card was used and whose key card it was.

- If you have temporary workers, volunteers, or student workers should have very limited access.
- If senior workers require access to storage and highly secured areas their key card should permit this.
- If non-employees, like contractors and consultants, are given access for special projects temporary key cards should permit access only to necessary areas and their movements should be monitored closely.
- If there is a bell for patrons to use for access to the special collections make sure it can be heard in the closed stacks so that staff will know that a user is seeking entry.

3.3 Lockers

Lockers are located just outside the entrance to the reading room. Patrons should leave backpacks and other belongings here while using the reading room. Lockers can either be coin return or use keys. If there are no lockers, a separate area should be designed for storing patrons' personal effects while they use the reading room.

Post a sign near the lockers/storage area and online noting what is allowed into the reading room.

3.4 User Registration

When a patron wishes to access special collections materials they must register as a researcher. This process includes providing picture ID, such as a driver's license or state ID, and filling out a form. The form should include fields such as what institution or organization the researcher is coming from, what their topic is and the purpose of their research (e.g. documentary, thesis paper, etc.).

3.5 Reading Room Practices and Policies

The reading room or reference area for the special collections should be laid out in manner that all working spaces are visible to the staff member at the reference desk. Any hidden areas should be visible to security cameras. The staff member manning the reference desk must monitor the camera and the tables.

Chairs should be placed at tables so patrons all face the same direction. Direct line of sight from the reference desk is best for prevention of theft and/or vandalizing of collections.

The list of rules for use of the reading room should be clearly stated and displayed on reading room tables or walls and should include the following:

- No food or drinks are allowed. Not even water.
- Cameras/phones are allowed but please do not use flash
- Bags, binders, folders and other personal effects are not allowed. Please place them in lockers available near the reading room entrance.
- No pens allowed. Only pencil.
- Laptops are permitted
- No gum chewing.
- Loose sheets of paper are preferred for note taking. Notebooks are permitted but will be subject to search upon leaving
- Materials in the special collections may not be checked out, they are for use in the reading room only.
- Please do not mark or erase markings in any books or on any documents.
- When using materials please use the proper supports to help keep them from breaking. Supports are provided by the institution.

3.6 Inspection of Materials Before and After Patron Usage

Before patron enters, make sure that they have only brought in appropriate materials.

Staff in the reference room should remain alert, watching patrons' actions and circulate the room periodically at random.

Upon the researcher completing their research examine their papers and folders to make sure they did not take any materials, whether by accident or on purpose.

Do not become lax with returning and regular researchers, especially those who are librarians or archivists.

Reading room should never be left unattended when a user is present and schedules should be set so that there is always at least one backup staff member available.

3.7 Identifying or Marking Collection Materials

Special collections should have some kind of marking or identification that links it to the institution such as discrete labels on acid-free, pH neutral paper attached with PVA.

When accessioning new materials each volume or item should be given a unique ID number written in a uniform place with pencil. Items without a preliminary inventory or finding aid should not be circulated or be loaned to or used by researchers.

Fragile items should be duplicated using a scanner or photocopier and duplicates placed for use by researchers. Duplicates should have a notation signifying that it is of duplicate status, a property mark and the collection number.

Digital copies should have a digital watermark embedded into the image and coding. This watermark should contain the date of creation and some kind of information that connects it to the collection. Digital copies should also be low resolution to discourage theft and publication without authorization or permission of copyright holder.

3.8 Disaster Response for Special Collections

Should there be disaster that causes physical damage to buildings, preventing entry, take extra care to secure collections. There are two choices post-disaster: 1) move collections to a secure storage away from damage (may be easier) or 2) have security guards patrol the area to prevent unauthorized access and further loss of materials (for larger collections).

Besides additional security and prioritizing treatment of special collections, follow normal emergency procedures for disasters (SEE EMERGENCY PROCEDURES CHAPTER).

4 Safety and Security of Electronic Files and Systems

Theft, tampering, and attack on library electronic hardware, software, and systems can cause financial burden to libraries, create issues pertaining to staff and patron privacy, and result in loss of institutional data. E-crimes can be difficult to detect, especially in the case of “stolen” files or data which remain with the “owner” but can be copied and used by others for various harmful purposes. Every library network system is vulnerable, to varying degrees. Good network security is expensive: perfect security is impossible. Anyone can sabotage or steal electronic files and systems, and in fact, the worst security breaches often originate internally. However, measures can be taken that can protect most of your equipment, software and data most of the time. However, there is often a tradeoff between high security measures and privacy of individuals. Below are some guidelines and procedures that ALL staff should be aware of and practice:

4.1 Know who to call

If there is a computer problem or if you suspect that someone is stealing or misusing library computers, software, or systems, use your phone tree to contact the IT department and the person in charge for your shift (SEE PReP template <http://westpas.org/workshop-docs/>).

4.2 Keep training current

Staff should attend all training sessions related to electronic and network security. They should become more knowledgeable about computer systems in an effort to be able to recognize when systems have been attacked or tampered with. Contact your department manager for opportunities for professional development in this area. Staff should be alert and observant in areas with computer and electronic equipment at all times. Staff should choose “strong” passwords (SEE SECTION 4.6), change passwords often, and keep password information secret and secure.

4.3 Hardware and peripherals

All monitors, CPUs, laptops, and peripherals including keyboards and mice at permanent computer stations should be locked down. Staff should periodically check and make sure that locking mechanisms are secure and report any problems to the IT department and person in charge.

4.4 Label all hardware and peripherals

Any equipment should be labeled with an ownership and identification number. This includes stationary and portable equipment (tablets, headphones, portable hot spots, etc.). This practice is necessary for proper inventory and insurance of electronic items. Management should make sure that all equipment is properly insured against theft and damage.

4.5 Use surge protectors

Make sure all library equipment is plugged in with surge protectors to protect equipment during power surges due to weather or building electrical problems. If you see missing surge protectors, notify person in charge and IT department.

4.6 Password protection

An aggressive password system is one of the lowest cost methods of network security and can be practiced by all libraries. All computer should have varying levels of password protection. Computers available for patron use should have guest passwords. Circulation desk terminals should have passwords that only circulation staff, management, and IT staff know. Office and Administrative terminals should have individual passwords that are only given to necessary employees. Train staff to choose “strong” passwords. Set passwords to expire periodically and reset them with another “strong” password. Delete expired accounts (e.g. when accounts are idle or when a staff member no longer works for the library).

4.7 Acceptable internet use policies

Require all patrons who request computer access to agree to an acceptable computer/internet use policy. This can be a required agreement before they are able to log in to a library computer terminal. The policy can also be posted on the library web site and retained in hard copy format near computer stations or at circulation desk.

Acceptable Internet Use policies may contain the following sections:

- Acceptable practices
- Unacceptable practices
- Time limits
- Modified rules/settings for children’s computers
- Consequences for misusing software/computers/network
- Disclaimers
- Notice of filtering
- Privacy statements

- Information about the USA PATRIOT Act
- Right of the library to discontinue access
- Copyright restrictions
- Any state or local statutes that apply to use or misuse of public computers and internet

Decide whether your institution will allow behavior such as downloading software and/or files and adjust computer settings and policies accordingly. Decide if and how you will limit patron time on computers and enforce your library policies. If you see a patron misusing the computers, you will need to file an incident report and notify the person in charge. A few examples of internet use policies are listed below:

Dallas Public Library

<https://dallaslibrary2.org/about/policy-computerAndInternet.php>

Multnomah County Library

<https://multcolib.org/policies-manuals/acceptable-use-internet-and-library-public-computers>

County of Los Angeles Public Library

<http://www.colapublib.org/aboutus/aupdear.pdf>

4.8 Access settings

Different terminals in your library should have different functionalities and access settings. Below is a sample of possible access settings your library may choose to use:

- OPAC (library catalog) use. These terminals may not require a password for use but they will neither have internet access nor access to other software programs (word, spreadsheet, email, etc.).
- Computers configured for internet access and/or access to software programs should be password protected with login information given only to the patron who has permission to use the computer at a particular time. These passwords should change frequently and terminals should delete browser history and reset to a configuration determined by the IT staff every time a patron ends a session.
- Functionality of the terminals in the children's area may be more limited and more aggressively filtered (see Filtering section below) than terminals in the adult area.
- Front Desk/circulation/reference computers should have password protection that only staff know. They should be configured to complete only the tasks necessary for the staff members at that service station. Though patrons may view information on these terminals, they should never be allowed to operate them without the direct and constant supervision of a staff member. Passwords for these terminals are not to be shared with patrons for any reason (see Password protection above).

- Office/Admin personal office computers will have more functionality than public computers. The user should have a “strong” unique password that very few people know (the individual, management, IT). They should be configured to access only the programs necessary for the staff member to complete their duties.
- IT staff should have the broadest access and knowledge of passwords. They should be able to change passwords and access settings and functionality of terminals and the network. However, once an IT person no longer works at the institution, all passwords should be updated so that that person no longer has access to the network.

4.9 Filtering

Some libraries are required by law to filter internet websites if they receive E rate funding for internet access. Libraries who do not receive E rate funding may still choose to filter some sites, for example at a terminal in the children’s section. However, whether a library is obligated or chooses to filter websites, a patron may request that a site be temporarily unblocked and the library should comply with that request. (SEE CIPA SOURCE)

4.10 Virus, Spyware, Malware

It is best practice to install virus, spyware, and malware protection on all of your institution’s electronic devices. Run scans on your equipment often and train staff to run scans, as appropriate. If you are not able to run a scan yourself, inform the person in charge and the IT department

4.11 Firewalls and partitions

Firewalls and partitions keep harmful information from penetrating your library’s network and/or confine malicious programs to a particular area of the network. This keeps others devices safe from the spread of a virus or vulnerability to a network attack. Firewalls and partitions can protect inside networks from outside networks or from other areas of the same inside network. Firewalls and partitions will likely be set up by the IT department. Do not disable firewalls or partitions and report any network problems to the person in charge and IT department.

4.12 Encryption

Encryption is a method of encoding information on your network. An institution might encrypt files, software, emails, data such as personal information, or all of the above.

Encryption makes it that much more difficult for someone to steal information or hack into your system. Encryption settings are likely to be set up and maintained by the IT department.

4.13 Electronic and paper waste

Deleted electronic files are never fully deleted but some types of “shredding” software are able to eliminate most digital data. Make sure your system has “shredding” software and that you use it. Likewise, paper documents can contain important patron or institutional information that may make your system vulnerable if they were to fall into the wrong hands. Therefore, make it a common practice to shred any paper document that contain identifying data or privileged information.

4.14 Backup

Your institution will want to retain some types of data. In those cases, make sure important data is backed up frequently and that backups are stored in different locations. That way, if the library sustains an unforeseen disaster, critical data will not be lost.

4.15 Share security breaches and solutions with other institutions

Communicate with other libraries about suspected or actual breaches in network security. You may find that other institutions have had similar occurrences or have found prevention solutions that you can also use.

References

- American Library Association. (2010). *The Children's Internet Protection Act (CIPA)*. Retrieved from <http://www.ala.org/advocacy/advleg/federallegislation/cipa>
- Chenoweth, R.M., Herring, S., Beach, S., Sayers, J., Westfall, M., Wilson, W.R., Brooks, J., Brandow, S., & Sherman, J.E. (n.d.). *Safe Harbor: Policies and procedures for a safe library*. Retrieved from <http://will.state.wy.us/ldo/boards/SafeWorkplace.pdf>
- Council of State Archivists (adapted by WESTPAS). (2006). *Template for Pocket Response Plan for Collections*. Retrieved from <http://westpas.org/workshop-docs/>
- County of Los Angeles Public Library. (2009). *Acceptable Use Policy*. Retrieved from <http://www.colapublib.org/aboutus/aupdear.pdf>
- Cravey, P. J. (2001). *Protecting library staff, users, collections, and facilities: A how-to-do-it manual*. New York: Neal-Schuman.
- Dallas Public Library. (2001). *Policies Computer and Internet Use*. Retrieved from <https://dallaslibrary2.org/about/policy-computerAndInternet.php>
- Department of Defense: Defense Civilian Personnel Advisory Service. (2012). *Preventing Workplace Violence for Employees*. Retrieved from <http://media.cpms.osd.mil/faslerd/employee/menu.htm>
- Department of Justice. (2010). 2010 ADA Standards for Accessible Design. Retrieved from <https://www.access-board.gov/guidelines-and-standards/buildings-and-sites/about-the-ada-standards/ada-standards/doj-s-2010-ada-standards>
- Department of Labor. (2016). United States Department of Labor Occupational Safety and Health Administration. Retrieved from <https://www.osha.gov>
- Graham, W., & Ebrary, Inc. (2012). *The black belt librarian: Real-world safety & security*. Chicago: American Library Association.
- Kahn, M. B. (2008). *The library security and safety guide to prevention, planning, and response*. Chicago: American Library Association.
- Louis, D. M. (1994, October 1). *Safety and Health Concerns in Academic and Public*

Libraries.

Multnomah County Library. (2012). *Acceptable use of the Internet and library public computers*. Retrieved from <https://multcolib.org/policies-manuals/acceptable-use-internet-and-library-public-computers>

Rutherford Public Library. (2011). *Procedures & Guidelines on Safety, Security and Disaster Planning*. Retrieved from <http://www.rutherfordlibrary.org/wp/wp-content/uploads/2011/06/Procedures-and-Guidelines-on-Safety-Security-and-Disaster-Planning.pdf>

Security in museums, archives and libraries: A practical guide. (2003). London: Resource.

Shuman, B. A. (1999). *Library security and safety handbook: Prevention, policies, and procedures*. Chicago: American Library Association.

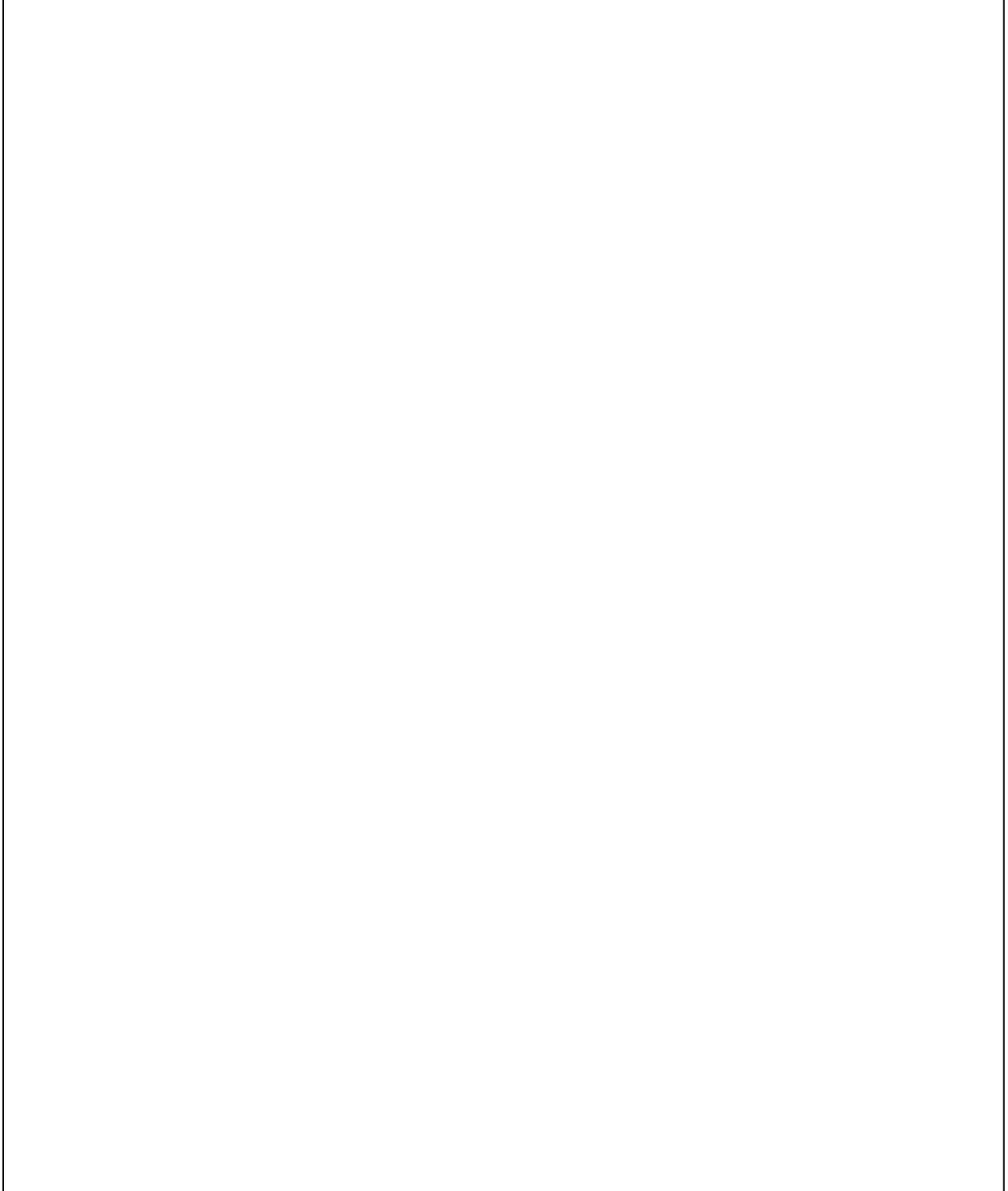
Texas State Library and Archives Commission. (2011). *Computer and Network Security in Small Libraries*. Retrieved from <https://www.tsl.texas.gov/ld/pubs/compsecurity/pthreepwdpol.html>

Trotta, C.J. & Trotta M. (2001). *The librarian's facility management handbook*. New York: Neal-Schuman.

Wilkie, Jr., E. (2011). *Guide to Security Considerations and Practices for Rare Book, Manuscript, and Special Collection Libraries*. Chicago: American Library Association Association of College & Research Libraries.

Appendix A: FLOOR PLAN

Insert floor plan here (add additional pages for additional floors if necessary):



Appendix B: ACCIDENT/INJURY/ILLNESS REPORT FORM

Date of accident/illness/injury _____ Time of incident _____

Full name of person involved in accident/injury/illness _____

Street _____

City and Zip Code _____

Phone number (include area code) _____

Age of person _____ Birth Date _____

Name of person's insurance carrier _____

Name(s) and address(es) of witness(es)

Summary of Incident (use reverse side if necessary):

Where did it occur?

What was the person doing when the incident occurred? Be specific.

Object or substance (source) responsible for injury:

Nature and extent of injury:

Action which was taken (i.e., ambulance called, person went home as desired):

Medical services called: Yes _____ No _____

Hospital name and address _____ Doctor's
name and address _____

Name of person filing report _____ Date of report _____

Date referred to Director _____

Appendix C: DAILY CLOSING CHECKLIST

_____ Minutes Before Closing: Make a general announcement over the intercom: “The library will be closing in _____ minutes. If you plan to check out books, please come to the desk soon. If you are using the computers or photocopier, equipment is turned off at _____ minutes before we close.”

_____ Minutes Before Closing: Repeat announcement with new time.

If you are unable to make a general announcement, someone in each department should remind everyone in the department that the library will be closing soon.

PROCEDURES:

_____ Minutes Before Closing:

One person from each department should walk around the department:

- Ask teens and unattended children if they need to arrange for a ride. The library makes the call if there is not a public pay phone.
- Remind customers that if they want to check out materials, they need to do so now while there is time.
- If customers are on the computer or photocopier, remind them that the library will be closing shortly and the equipment will be turned off _____ minutes before closing.
- Step into the restroom (or if a single use facility, knock on the door) and say the library will be closing soon, please prepare to close.

While doing this, a designated person may also:

- Check that unused equipment is turned off, if appropriate. This is especially important for heaters, fans, and equipment in workrooms and offices.
- Pick up books and papers, left on tables and shelves. They should neaten as they walk.
- Check restrooms for occupancy and if empty, turn off the lights. Make sure all toilets are flushed and that there are no messes that need addressed. Note problems for the custodians.
- Check all rooms, closets, and storage areas. Lock doors as rooms are checked.
- Check that all windows are closed and locked.

_____ Minutes Before Closing:

- Turn off computers, photocopiers, and other equipment.
- Lock more doors. If multi-floor building, lock doors to entrances to other floors. Crash bars should still allow egress.

At Closing:

- Walk up and down the stacks to make sure everyone is out.
- Check the restrooms again. Turn off lights when everyone is out.
- Check all rooms, closets, and storage areas.
- Lock doors if you have not already done so.
- Put money away(after all patrons are out and building is locked).
- Make sure all equipment is turned off or disconnected if appropriate.
- Activate alarms, if appropriate.
- Everyone leaves at once for the parking lot. This ensures that no one is inadvertently left in the building with the alarms on and promotes safety in the parking lot.
- Note non-staff vehicles still in parking lot. Write down license plates in an incident report or follow suspicious behavior procedure (SEE SUSPICIOUS BEHAVIOR).
- Note non-staff still in parking lot. If appropriate, document in an incident report.

Appendix D: SAFETY AND SECURITY CHECKLIST

Date checked:

Conducted by:

	YES/NO	COMMENTS
Are locks secure at all entrances/exits/offices?		
Are aisles and passageways clear?		
Are walking surfaces safe and slip resistant?		
Are any exits blocked?		
Are emergency numbers posted at all public service areas/staff lounge?		
Is disaster manual located in an accessible place?		
When was last inspection by Fire Department?		
Fire extinguishers available and up to date?		
Fire alarm tested recently?		
When was the last fire drill?		
All smoke detectors operable?		
Public address system operable?		

Emergency/Exit lighting operable were needed?		
First aid kits available/well stocked?		
Cellular phone service available?		
Are all staff members familiar with the location of emergency equipment, flashlights, first-aid kits, shutoff valves for utilities?		
Any other lighting issues?		
Are all chemicals properly labelled/stored?		
Any indication of possible leaks?		
Any worn or exposed wiring?		
Any overloaded sockets?		
Any ungrounded equipment?		
Are restrooms in sanitary and working condition?		
Any potentially unsafe condition?		