NEDCC
NORTHEAST DOCUMENT CONSERVATION CENTER

PRESERVATION LEAFLET

EMERGENCY MANAGEMENT

3.11 Collections Security: Planning and Prevention for Cultural Heritage Institutions

INTRODUCTION

Many cultural heritage institutions fail to recognize the vulnerability of their collections to loss. Collections can be threatened by theft and vandalism, disasters (e.g. fire or flood), and damage from careless handling or poor environmental conditions. Any institution seeking to provide the best possible security for its collections must put in place coordinated policies that address all of these threats. Since NEDCC's Preservation Leaflets on The Environment, Emergency Management, and Storage and Handling can be consulted for information on disaster planning, environmental control, and proper storage and handling, this leaflet will focus on problems associated with collections security: theft and vandalism.

Most cultural heritage staff members have heard stories describing trusted patrons, relative strangers, or even valued staff who have pilfered collections (for personal gain or to add to private collections), but many do not believe such things could happen in their institution. Too often staff and management do not recognize the occurrence or the effects of theft and vandalism, and while most institutions have basic security policies, consistent enforcement can be difficult to achieve. Some patrons, and indeed some staff, see security measures as unnecessary inconveniences.

If a security program is to be effective, there must be widespread understanding of the importance of security to the mission of the institution: fundamentally, missing or damaged collections cannot be made available for use. It is important to understand that while some damage or loss can be ameliorated (for example, a stolen journal might be replaced through purchase, books missing in one library may be loaned from another, or missing pages may be photocopied), other materials are irreplaceable if the material is unique, rare, or difficult and expensive to replace.

This leaflet will discuss strategies for preventing theft and vandalism of collections, responding to any breach of security that might occur, and creating an effective, universally enforced security plan.

SECURITY PLANNING

If collections are to be protected against loss, cultural heritage institutions must consider security as a management issue deserving an investment of resources. Security planning must be supported at the highest level of the institution. A collections security plan will be most effective if it is coordinated among the various departments and/or areas involved in maintaining security. Such coordination can be a challenge, so long-term institutional commitment is essential. Activities that may have a security component include collection storage, cataloging or processing, circulation, reference services, special events, building maintenance, staff training, insurance, and conservation services.

Basic Components of Security Planning

1. Prepare a written security plan. If appropriate, form a security planning committee to help develop policies and procedures.
2. Appoint a security manager to develop and implement your security plan.
3. Perform a security survey to assess your needs.
4. Initiate preventive measures:
   - Eliminate weaknesses to ensure the security of the building.
   - Install appropriate security systems.
   - Ensure that collection storage is secure and that good records are kept.
   - Establish patron regulations.
   - Establish staff regulations.

5. Plan your response to any breach of security. Document the steps staff should take and practice response plans.

6. Maintain and update your security plan.

Each of these planning elements are discussed in more detail below. While specific security measures may differ from institution to institution, depending on size and available resources, this planning process is appropriate for any organization.

1. THE SECURITY PLAN

Every cultural institution should develop a written security plan that articulates its commitment to security management. Many of the principles for writing and maintaining an emergency preparedness and response plan (a "disaster plan") will also apply to preparing a security plan; in fact, in most institutions these two plans will be closely related. (NEDCC Preservation Leaflets on Emergency Management provide additional information related to preparing a disaster plan.) An important part of the security program will be regularly reviewing and updating the plan (see #6 below).

When preparing a security plan, the first step is to appoint a security manager to put together a security planning committee. (See #2 below. In a small institution this may be a committee of one.) This committee will perform a security survey (see #3), identify preventive measures (see #4), and write a security plan. This committee must have the institution director's authority to act. With this endorsement, the committee can invite staff in all areas of the organization to contribute to the draft plan.

The security plan should include the following:

- A statement supporting security planning, prevention of incidents, and the implementation of response procedures;
- Definition of the security manager's responsibilities;
- Information about security systems in the building;
- Information about distribution and control of keys to the building and to any special storage areas;
- Copies of all policies and procedures relating to security (patron and staff use of the collection, collection management policies, etc.);
- A checklist of preventive measures to be undertaken;
- A list of procedures for responding to a security breach (see #5 below).

Remember that it may not be appropriate to include some of this information (e.g. security system information and key control information) in all copies of the plan. While all staff members should have a copy of the security plan, some of this information should be limited to upper-level staff members.

Always ensure that the plan is endorsed at the highest managerial level and shared or coordinated with local police and related officials. All copies of the plan must be stored in areas where they cannot be accessed by the general public.

2. THE SECURITY MANAGER

A security manager should be appointed to coordinate security planning. In smaller institutions, a staff member may be assigned this responsibility along with many others; in a large institution, this might be a full-time position. Particularly in the case of a part-time security manager, security responsibilities should be clearly stated and incorporated into the staff member's job description. A certain amount of time should be set aside for that person to work on the security program. The security manager should prepare regular assessments of the program and work to improve systems and procedures as needed.

The security manager will need to work with all staff members that have contact with the collection. As noted above, these areas might include collection storage, cataloging or processing, circulation, reference services, special events, building maintenance, staff training, insurance, and conservation services. The security manager must have direct access to the institution's director and sufficient authority both to coordinate preventive efforts among the staff and to act during a security emergency.

3. THE SECURITY SURVEY

Before initiating or upgrading a security program, an assessment of current and projected needs is recommended. The security manager, together with the security planning committee, if any, should make a systematic study of the facility and its operations.

This survey should evaluate current security policies and procedures, identify potential areas of risk, and rank security threats according to the probability of occurrence. This will allow the institution to concentrate on the most serious problems first, and it will assist in long-term planning and budgeting.

A survey looks at the following: 1) external perimeter and interior areas for inadequacies, such as proximity to other facilities which pose a risk, inappropriate intrusion detection and signaling, poor lighting, poor sight lines, and inadequate locks; 2) current policies and procedures for use of the collection by staff and patrons, including patron registration, reading room procedures, staff access to the collection, and key control; 3) collection protection in storage, in transit, and on exhibition; and 4) any past problems and concerns identified by staff or others. See "Further Reading" for examples of security surveys and checklists.

4. PREVENTIVE MEASURES

Once a survey has been completed, it is likely that improvements in preventive security measures will be needed. Activities designed to prevent loss or damage fall into several categories: external and internal building security, patron regulations, and staff regulations. Each will be addressed below.

Building Security

The building and collection must be secured both during and after normal working hours. Unauthorized entrance to the building and unauthorized removal of collection material from the building must be prevented.

The perimeter of a building can be protected in various ways, ranging from the use of door and window locks to more expensive strategies like the posting of security guards and/or installation of an automated security system.

Internal building security is important both during and after working hours. Most institutions should have a secure room to protect valuable items when they are not being used; this room should be secured even when the institution is open, and the number of personnel having access should be strictly limited. Valuable materials should always be stored in this room when the institution is closed.

Automated security systems are discussed separately in the following section. Other strategies for upgrading building security include:

- Installing high-quality, heavy-duty locks, dead bolts, and hinges on all exterior doors.
- Installing grilles or screens on ground-floor windows.
- Requiring patrons and staff to enter and exit the building by one door, which is monitored at all times.
- If appropriate, installing a book security system. (This is NOT appropriate for rare or unique materials such as those found in archival and historical collections. It is normally used for general circulating collections.)
- Storing valuable collections in a locked room and limiting access to the key, instead of locating collections in open stacks or a building with easy public access. Ideally, the room should have no windows, a solid door that opens out, a minimum one-inch dead bolt, and pinned hinges. Door buzzers and alarms are recommended.
- Employing one or more security guards to patrol the institution after closing.
- Ensuring that alarms (e.g. fire) are always secured, tamper proof, and located away from the main stream of traffic to prevent accidental false alarms or deliberate use of an alarm to distract from a theft in progress.
- Taking steps to prevent removal or duplication of keys, ensuring that keys are returned when employees leave, and changing all locks periodically.
- Installing after-hours security lighting.

Security Systems

An automated security system serves three main purposes. First, the mere presence of a system can act as a deterrent to crime. Second, if an intrusion occurs, it will be detected. Finally, the system will notify appropriate personnel, making apprehension of the intruder more likely.

There are additional advantages: modern alarm installations are relatively inexpensive; other alarms (water alert, fire, power outage, temperature) may be connected to the security control panel; an alarm system can provide two-way communication (opening and closing of gates, arming devices, etc.);

recorded data can be used to produce management logs (status summaries, alarm summaries, entry and exit reports, etc.), and most systems are expandable, so it is possible to start with the basics and enhance the system later.

Despite these advantages, an automated security system should never be an institution's only protection. Since **most thefts occur during working hours and occur because of human errors**, it is essential to have a broad-based security plan that also includes strategies for protecting collections during use. (See the following sections on patron and staff management.)

How Security Systems Work

A basic security system will secure vulnerable perimeter access points such as doors and windows, and it will protect interior spaces via interior motion detectors that monitor movement inside the premises. An electronic security system includes sensors, a control panel (which interprets the report from the sensors and decides whether or not to activate the reporting devices), and reporting devices (which might be a traditional alarm or a signal to a security company monitoring the system).

In order to ensure response to an alarm, you must have the security system monitored 24 hours a day by the monitoring station. If you use a local signal only, you must rely on a neighbor to call authorities when the alarm sounds. Costs for a monitoring system normally include a monthly fee and can be arranged through your alarm installation company. While there are a number of companies that install and monitor their own accounts, there are many more that install systems and contract with a third-party monitoring facility.

How to Contract for a Security System

Remember that alarm companies tend to concentrate on night-time protection, without any thought to a public institution's vulnerability during daytime visiting hours. If your security survey has been completed and the findings incorporated into your plans, you will be better prepared to discuss specific needs and design options with the alarm company.

A great deal can be learned about a company through its sales representative. A sales representative should be knowledgeable about all areas of the alarm industry. It is this person's job to customize a system that will provide the level of protection needed with as little disruption as possible to the facility. This can generally be accomplished through an effective system design.

A qualified company will perform a site inspection and discuss your individual security needs before installing a security system. Each institution is unique, and the system should be tailored to fit your needs and price range. The company should provide you with an evaluation of your premises, highlighting the measures you can take to improve the security of your institution over and above the addition of an electronic alarm system.

When comparing companies, be sure to make a true comparison by thoroughly reviewing the number and types of products being installed. After installation, carry out periodic tests of the system to ensure that it is in proper working order at all times.

Do-it-Yourself Security Systems

For smaller or less well-resourced institutions, contracting with a security company to install and monitor a system may be too expensive. In these cases, a “do-it-yourself” (DIY) security system that the purchasing organization installs itself is a viable option. Self-installed systems offer the same functionality as a traditional system, but they are generally less expensive, do not require a contract, and have flexible monitoring options. Any institution considering a DIY system will need to fully understand its advantages and disadvantages.

Because the purchasing organization must set up the system, a company representative will not visit the site. Staff at the institution will be responsible for assessing security needs and selecting and installing equipment without the guidance of a professional. It is possible that staff will miss vulnerabilities and place sensors ineffectively.

Many DIY systems also allow institutions to choose between professional monitoring and self-monitoring and to switch between these options as needed. To save on monitoring costs, an organization can designate specific staff to be on call for responding to security system alerts and schedule professional monitoring only when staff are unavailable. An organization should keep in mind that no matter how attentive staff members are, self-monitoring results in a greater chance that an alert may be missed.

The challenges of self-monitoring and self-installation become more significant at scale. The greater the number of entryways to a building, then the more difficult it will be for staff to install the system. Additionally, the higher the amount of foot traffic in and around the building, then the more demanding it will be to ensure staff respond to every alert, including false alarms.

Evaluating these risks and drawbacks against the cost-saving potential will be essential to an institution's decision-making process. If managed properly, a self-installed system in a small organization will bolster security, and an organization that has conducted a security survey and developed a security plan will be best prepared to adopt a DIY system.

Security Guards

The use of security guards may be appropriate in some situations. All staff members (including general staff, management, custodial workers, grounds keepers, and volunteers) will still need to participate in maintaining security, but guards can be a valuable supplement to staff efforts, and their presence alone may deter theft and vandalism.

It is important for an institution to specify its needs, communicate them clearly to the security guards, and supervise those personnel. This is true especially if services are contracted from a private company. It may also be advisable to incorporate incentives and penalties into the contract to ensure that services are performed satisfactorily. The security manager must determine what equipment, instruction, and supervision the security personnel will receive. It is important to work with guards to develop a daily schedule for monitoring the institution's activities and a mechanism for making regular reports.

Collection Management and Security

Collection management is an important aspect of security. It is difficult to verify that something is missing if collections are not properly cataloged. In the case of theft, inventories and identification marks can help prove an object is the item in question and provide proof of rightful ownership. Detailed collection records can also help the collection curator separate intrinsically valuable items for secure storage or other special treatment. In addition, regular inventory of collections can identify missing items that might otherwise have been overlooked.

Specific collection management activities that will be helpful in maintaining security include:

- Inventory your collection on a regular basis.
- Ensure that storage areas are arranged for quick and easy inspection.
- As materials arrive in the institution, identify and segregate valuable and/or marketable materials (monetary or intrinsic value). Store valuable and/or marketable items separately in a secure area and consider substituting photocopies or photographic reproductions for the originals for access purposes.
- If valuable and/or marketable items will not be stored separately, place them in separate folders within the collection so they can be easily checked by a staff member. Create procedures to ensure the collection is inspected for completeness before and after use.
- Record a physical description of valuable materials to aid recovery and ensure positive identification should a theft occur.
- Protect catalog records and finding aids by maintaining off-site backups and ensuring no staff member can destroy these records on their own.
- Provide insurance coverage for valuable materials.
- Consider using some form of identification mark for the collection. This may not be an appropriate choice for materials with artifactual value but may be useful in some situations.
- Use call slips, sign-out sheets, computer systems, etc. to record and track the use of the collection during research, loan, exhibition, conservation, digitization, etc.
- Do not allow patrons access to unprocessed collections.

Patron Management

Collection curators must maintain healthy patron relations while enforcing reasonable rules and procedures. It is unfortunate that there are many documented cases of "regulars" and trusted professionals being given privileged access to a collection and then violating that trust by stealing from the collection. Such researchers are often allowed to work without supervision and regular checking of personal effects or the materials being used. It is only later that the institution discovers a pattern of loss, often of the most valuable items. It is essential to remember that the safety of the collection must come first. The great majority of patrons will understand and abide by rules and procedures once the reasons for them are explained.

The cornerstones of managing the use of archival and special collections are supervision of patrons; inspection of patron belongings and of collection materials (before and after use); and the maintenance of records documenting the use of materials. Supervision and inspection will help to prevent theft and vandalism, and records that document use may be invaluable in a theft investigation. If all of these activities are carried out routinely, patron use of collections can be well managed in even the smallest institution.

The following procedures apply to use of collections in an institution with a separate reading or research room, rather than to use of general circulating collections:

Patron Access: Step-by-Step

1. All patrons must be required to register:
   - Each patron should complete a Registration Form that asks for identifying information and information about research interests, and each patron should sign a logbook. A sample registration form is included at the end of this leaflet.
   - All patrons should be required to present photographic identification when they register. A staff member should monitor the registration procedure to ensure that the name appearing on the identification matches the one given on the registration materials.

2. If desired, a photographic ID may be retained from each patron until the research materials are returned. The ID should be attached to the completed registration form and stored in a secure place. At a large institution, in-house ID might be issued for regular users.Perform a reference interview:
   - Record each patron's interests.
   - Discuss their research topic and evaluate their request.
   - Determine the amount and scope of materials that will meet the patron's needs.
   - Scrutinize the patron's intentions.
   - Explain finding aids, catalogs, and services.

3. Explain the rules for use of materials:
   - Allow only necessary research materials into the reading room. The institution should provide lockers or other secure storage for the personal effects of patrons (coats, briefcases, purses and oversize handbags, portfolios, etc.).
   - Containers and personal effects that are allowed in the reading room should be separated from the tables.
   - Do not allow patrons to use boxes or laptops to obstruct the view of reading room staff.
   - Provide written guidelines for proper handling of materials (e.g. use book supports, use pencil instead of pen when writing, etc.).
   - Remind patrons to keep materials in the order in which they are found. Limit the number of boxes patrons can use at one time. Instruct patrons to put materials away each time they leave the reading room.
   - Explain how to use call slips. All collection materials that are retrieved must have a slip, and patrons should be required to sign the slip(s).
   - Require patrons to sign a form stating that they understand and agree to comply with the rules for handling and use. A sample form of procedures for researchers is included at the end of this leaflet.

4. Ensure that the reading room is adequately staffed at all times. Ideally there should be two staff members so that one can retrieve materials while the other supervises the patrons.

5. Check each archival box for collation and completeness before and after it is used by patrons.

6. Each time the patron leaves the reading room, inspect any personal materials that were allowed into the room.

7. Inspect collections for sequencing and completeness before re-shelving. A retention schedule should be established to ensure that registration forms and call slips are available if they are needed later for investigating a theft. Determine how long these records will be retained.

Patron Access in Small Institutions

The recommendations given above may seem difficult if not impossible to implement for small institutions with few staff members, such as historical societies (which are often staffed by volunteers) and public libraries (which are often responsible for managing both circulating and historical collections). With some effort and institutional commitment, however, reasonable security can be provided even in a situation where staffing limitations make constant supervision of researchers difficult.

No matter how small or understaffed the institution is, patrons should be required to sign in and a record should be kept of the materials they use. It is a good idea in situations like this to retain identification from the patron until they are finished working. This makes it less likely that they will leave the building with items from the collection. A secure locked drawer must be provided for storage of identification.

Regarding supervision, it is most important to provide an area where readers can be watched while they are working and where it is difficult for them to leave the building unobserved. In a historical society, patron visits should be scheduled when a volunteer is available. In a library where supervision cannot be provided in the special collections reading room, patrons should be required to work at a table in view of the general reference desk or other library personnel.

In a situation where constant supervision cannot be provided, it is crucial to check patrons' belongings when they exit the building and to inspect archival materials before and after use. This can be awkward, but it will be easier if the procedures and the reasons for them are clearly explained to patrons at the outset. Institutions are advised to get counsel to ensure full compliance with laws regarding privacy, search, and seizure. For historical book collections that do not contain unique or rare material, the use of a book security system may also be helpful. Remember that the purpose of these procedures is not to inconvenience patrons, but rather to safeguard your collection and demonstrate to your patrons that these materials are important to your institution.

Staff Management

Involving all staff in planning efforts will increase the likelihood of an effective and smoothly-run security program. Staff members who work with the public are an excellent source for input on how to improve security procedures, and they should be encouraged to contribute their ideas.

Training staff members to implement the security plan is essential, since the primary reason security procedures are not implemented is that staff members find it awkward or inconvenient to do so. All staff must be instructed to enforce all rules, regulations, and procedures without exception. If exceptions are made routinely, a lax atmosphere conducive to theft and/or vandalism can develop. Staff should be trained in the techniques of observation. The room supervisor should move around the reading room on a regular basis to observe as well as to provide assistance to the researchers. All chairs in the reading room should be facing the reading room supervisor and with clear sight lines. Chairs on both sides of the table make observation difficult.

While the importance of universal enforcement of security procedures must be communicated to staff, it is also essential that staff are trained to deal with difficult situations that can make security procedures difficult to enforce. What should a staff member do if a patron refuses to provide registration information? If a patron refuses to have his/her belongings inspected? If a patron mishandles collections while working with them? If the institution does not have a professional security staff, it is a good idea to bring in a security professional to address these issues in a training session.

Unfortunately, another aspect of staff management is the protection of collections from theft by staff members themselves. There are some basic precautions that can be undertaken. Staff backgrounds can be checked before hiring; staff access to restricted areas can be limited; key control can be strictly enforced; staff belongings can be inspected when staff members exit the building; and staff can be required to sign in and out of the building, both during and after hours.

5. RESPONDING TO A SECURITY PROBLEM

It is important for a security plan to include procedures for responding to a security breach. This might be a loss that is discovered after the fact or it might be a theft in progress, and it might involve a researcher or even a staff member who is behaving suspiciously. In all cases, the goal should be to recover the missing materials and to apprehend the person responsible. The success of this effort will depend on quick action.

Some general guidelines are given below. (These guidelines are discussed in more detail in Chapter 8, "Crisis Management," in Gregor Trinkaus-Randall, *Protecting Your Collections: A Manual of Archival Security* (Chicago: Society of American Archivists, 1995.) In addition, it is essential that you speak with local law enforcement before writing your own procedures. Local law enforcement can explain when it is appropriate to contact them or a state or federal agency, what information you should have when police arrive, and how to respond to a situation when the suspected perpetrator is still on the premises, including whether or not you can temporarily detain the individual until police arrive.

Theft by a Patron

If a staff member suspects a patron of theft and if time allows, the staff member can consult with security personnel or police on how to proceed. Generally, no independent action should be taken unless the staff member actually sees the theft or discovers that materials are missing in the process of checking them before and after use. In that case, the staff member should request that the patron to step into an office or other area away from the reading room. If possible, a second staff member should accompany them so that there is a witness. It is important not to touch or to coerce the patron. If the patron agrees to be detained, notify and await the arrival of security personnel or the police. If the patron insists on leaving, one staff person should notify the authorities and the other should carefully follow the patron to get a description of the patron's car or direction of travel. In any case, staff should write down all pertinent information as soon as possible, in case it is needed for future legal action.

Theft by a Staff Member

Some of the warning signs that might indicate theft by a staff member include: one person consistently reports items missing or frequently finds missing materials; attempts have been made to alter collections records; a staff member frequently requests exceptions to the institution's rules and regulations; and a staff member appears to have a lifestyle that does not match his or her known resources. If a staff member is suspected of theft, determine the procedures to be followed before approaching the person. Typically, the person should be confronted by at least two supervisors and given a chance to explain his or her actions. It may be necessary to remove the person from the department temporarily and/or to contact police or security personnel.

After the Fact

It is somewhat more likely that a theft will be discovered after the fact, making it more difficult to identify the perpetrator. In such a case the security manager might choose to contact the police for advice on how to document efforts to determine exactly what is missing. (These might include an inventory of the collection if multiple items are involved.) Contacting the insurance company and reporting missing, recovered, or forged material to other appropriate organizations, such as the Antiquarian Booksellers’ Association of America, comes next. All actions taken to locate missing materials and identify the thief should be carefully documented both for future legal action and self-assessment.

Following an actual or suspected security problem and activation of any part of the security plan, the security manager should conduct an After Action Review (AAR) to discuss what happened and to evaluate the effectiveness of the security plan. (See “Further Reading” for more information about AAR.)

6. MAINTAINING AND UPDATING A SECURITY PLAN

Once the security plan is finished, do not allow it to gather dust on a shelf. The security manager should review it annually with all staff to ensure that everyone, including those newly hired, is familiar with its contents and has practiced response procedures.

Minor updates to the plan will be needed when basic information changes, such as the contact information for the security system vendor. More extensive updates will be needed in other situations. Following activation of any part of the security plan, the security planning committee should discuss the security manager’s After Action Review and update the security plan to strengthen it. In addition, the committee should conduct a new security survey whenever needed—for example, following a building renovation or collection move—and revise and improve the plan as necessary. Be certain to share the updated plan with police and related officials with whom you have shared your previous plan.

CONCLUSION

It is an unfortunate reality that cultural heritage institutions must be concerned about the security of their collections. It is recommended that all such institutions conduct a security survey and draw up a security plan. While there is a place for automated security systems of various types, an institution must not depend solely on these systems to protect its collection. Its security plan must also include policies and procedures regulating access to the collection by staff and users; mechanisms for identifying missing items; and procedures for responding to a security breach. Most important, the institution must recognize the difficulties staff members can face in enforcing security policies and provide training that will reinforce the importance of security activities and give staff members the skills they need to carry out these important duties effectively.

FURTHER READING

ACRL/RBMS Guidelines Regarding Security and Theft in Special Collections, American Library Association, October 5, 2009. http://www.ala.org/acrl/standards/security_theft (Accessed November 22, 2019). Document ID: 23c968f7-d77b-9514-0d72-b603f2931377. Anyone entrusted with the care of valued library materials should review this document thoroughly.

Albrecht, Steve. *Library Security: Better Communication, Safer Facilities.* Chicago: ALA Editions, 2015. Includes a security assessment checklist.

Fennelly, Lawrence J., ed. *Effective Physical Security*. 4th ed. Boston: Butterworth-Heinemann, 2013. An invaluable resource detailing the essential components of a secure facility, including security hardware and systems.

LYRASIS. “Security Audit.” A comprehensive checklist in the LYRASIS Preservation Services Leaflet series. https://www.lyrasis.org/services/Documents/General%20Preservation/Security-Audit.pdf

Museum Association Security Committee. http://www.securitycommittee.org. Though dated, this unofficial website of the security committee for the American Alliance of Museums includes articles on a range of topics.

Robertson, Guy. "The Elvis Biography Has Just Left the Building, and Nobody Checked It Out: A Primer on Library Theft." In *Robertson on Library Security and Disaster Planning.* Waltham, MA: Chandos Publishing, 2016. Written with humor, the author describes various techniques for stealing from libraries and archives, then lists basic (and mandatory) preventive measures.

Salem-Schatz, Susanne, et al. “Guide to the After Action Review,” version 1.1, October 2010. https://www.cebma.org/wp-content/uploads/Guide-to-the-after_action_review.pdf (Accessed November 22, 2019).

Shuman, Bruce A. *Case Studies in Library Security*. Westport, Conn: Libraries Unlimited, 2002.

Society of American Archivists’ Security Section. https://saasecuritysection.wordpress.com/ A blog and bibliography.

Trinkaus-Randall, Gregor. *Protecting Your Collections: A Manual of Archival Security*. Chicago: The Society of American Archivists, 1995. https://hdl.handle.net/2027/mdp.39015034282304 (Accessed November 22, 2019). An invaluable primer for developing an effective security program, including enough detail to implement the basics.

U.S. Federal Bureau of Investigation. "What We Investigate: Art Theft." https://www.fbi.gov/investigate/violent-crime/art-theft (Accessed March 30, 2020). A list of federal laws relating to cultural property theft.

Wilkie, Everett C., Jr. *Guide to Security Considerations and Practices for Rare Book, Manuscript, and Special Collection Libraries.* Chicago: ALA Editions, 2011. This volume focuses on the prevention of theft of rare materials.

Willoz-Egnor, Jeanne. "Mysterious Disappearance: Where's my stuff?" The Mariner's Museum, May 2013. https://www.marinersmuseum.org/blog/wp-content/uploads/2013/06/Mariners-Museum-AAM-handout-1.pdf (Accessed November 19, 2019.) This is a detailed case study about theft by a staff member with lots of tips for prevention.

SAMPLE PATRON REGISTRATION FORM

Name of Institution: ____

Location: ____

Mailing Address: ____

Telephone Number: ____

Email address: ____

Researcher Registration and Procedures

1. Please sign the registration book each day you use the reading room.
2. Please complete the following, read the procedures, and sign the agreement below.

Name (print clearly): ____

Identification type and number: ______________________________

Mailing Address:

____

____

____

Current Local Residence:

____

____

____

Professional Affiliation:

____

Subject of Research:

____

____

The following procedures must be observed while conducting research in the Archives. You must sign the statement agreeing to abide by these procedures. They are intended to allow access to the collections while preserving them for future generations.

SAMPLE RESEARCHER PROCEDURES

- Coats, parcels, purses, backpacks, briefcases, and other similar belongings must be left at the coat rack in the lobby, or in the lockers provided.
- No documents are to be removed from the research area under any circumstances. Archival materials are never loaned but must be consulted in the archives.
- All food and beverages must be consumed only in designated areas. No smoking anywhere in the building.
- Up to three boxes of materials can be requested at any time, but only one box at a time can be used by the researcher to ensure that materials are not placed in the wrong box.
- Original documents are not made available to the researcher if a copy (microform, photocopy, digital image, etc.) is available.
- Original order must be maintained within each box and within each file folder. If you have a problem returning items to original order, or if you find something out of order, please consult a staff member.
- Misconduct or disrespect of the rules may result in the researcher's being refused further access to the Archives.

By affixing my signature below, I certify that I have read the list of procedures, and that I agree to abide by said procedures in any use I make of the collections at the (Name of Institution).

Signature: ____________________________ Date: ______________

Collections used: ____

Staff member on duty: _____________________________________

ACKNOWLEDGMENTS

Written by Karen E. Brown and Beth Lindblom Patkus (1999). Revised and updated by Ann Marie Willer and Sean Ferguson (2020).