Section 5

Security

5.1 - RATIONALE

Security systems are critical in archival facilities to protect the facility and its irreplaceable collections from destruction, terrorism, vandalism, theft, unauthorized access, unauthorized alteration, and other threats.

Because an essential prong of comprehensive archives security is a vigilant staff who makes protecting archives facilities and the records a top priority, security systems and procedures in archival facilities are best when they are designed to empower the staff and minimize the opportunities for adverse actions against the facility and its holdings. Therefore, establish a design that includes layers of security from the exterior to the interior addressing:

- Site and perimeter
- Building envelope
- Building interior
- Building automation system
- Public areas
- Secure staff areas
- Collections storage
- Information technology (IT)

Archival facilities and their budgets vary, as do their security needs. Additionally, security technology is continuously evolving. With careful analysis, choices for security should be based on the feasibility, appropriateness, and longevity of the security program for the facility and collections. Even if all of the measures are unattainable by a small repository, every possible measure taken will be a step toward the ultimate goal of better protecting the records stewarded by the archives.

5.2 - SECURITY RISK ASSESSMENT

Also known as a security risk analysis, an assessment examines the exterior and interior of the facility, as well as aspects of the archival operations and procedures. It guides the design and security recommendations for the entire facility. Because no two archives are identical, it is imperative that each institution performs such an assessment. The security risk assessment includes an evaluation of:

- The exterior site
    - Roads
    - Alleys
    - Entrances
    - Parking lots
    - Landscaping
- The building envelope
    - Doors
    - Windows
    - Emergency exits
    - Ventilation openings (grates, ducts, shafts)
    - Exterior lighting
- Interior spaces
    - Collections storage rooms
    - Exhibit spaces and exhibit cases in non-exhibit spaces
    - Processing rooms and labs
    - Research rooms
    - Public areas
    - Corridors
    - Loading dock and receiving areas
    - Mail rooms
    - Offices and administrative spaces
- The digital/electronic security infrastructure
- Security policies and procedures

The security risk assessment takes into account specific guidelines mentioned in 5.3 through 5.10.

5.2.1 - Security Plan and Procedures

Standard Operating Guidelines (SOPs) or Standard Operating Guidelines (SOGs) are necessary to maximize the effectiveness of security systems.

- Address all security scenarios from theft to full failure of building systems and provide instructions for how to respond in each situation
- Includes:
    - a listing of possible emergencies and procedures
    - steps to take initially
    - whom to notify
    - doors to monitor and/or lock
    - lights to turn on

5.3 - EXTERNAL SECURITY

Design the facility's external security to mitigate risks and address its site and location and to meet all applicable codes and regulations.

- Design all means of access to the facility against unauthorized entry into the facility.
- A location near police and fire services can provide a short response time in emergencies.
- A location near a strategic military installation or symbolic site could place the archival facility in an area targeted in armed conflict, a terrorist attack, or civil unrest. Refer to Section 1.2.1 for additional guidelines regarding site hazards.

5.3.1 - Perimeter

Secure the perimeter and all access to the facility against unauthorized entry and vandalism.

- Clear view of all entrances and any architectural feature that could be used to gain unauthorized entrance to the facility
    - Avoid landscaping that can obstruct views or hide a person
- One public entrance
- Clear illumination with vandal-proof lighting during dark hours and an emergency power back-up
- Provide an intrusion detection system, covering all doors, windows, and other openings monitored by a Central Monitoring Station
    - A back-up electricity source is necessary in the event that the security system's main source of power goes out.

Optionally, a repository can include:

- Monitored and recorded video surveillance for parking areas and pedestrian walkways.

In some instances, a buffer zone with increased security measures around the repository is necessary. When appropriate, such a perimeter can include:

- Fences
- Walls
- Natural barriers
- Security gates
- Screening area for delivery trucks

5.3.2 - Windows

Windows, although aesthetically appealing, present security risks to archival facilities and their collections.

- Collections storage rooms
    - Ideally no windows
    - If there are windows, take measures to secure them and block light
    - Avoid skylights
- Exhibits, Processing rooms, Labs, Research rooms
    - Secure windows
    - Double glazed and filtered against ultraviolet radiation
    - Avoid skylights
- Other areas including offices, conference rooms, pubic areas, etc.
    - Secure windows

If windows or skylights are accessible from the exterior, consider bolstering the security of the windows to include bars, grills, metal shutters, glass break detection sensors, motion detection sensors, or a combination of such measures.

5.3.3 - Exterior Doors

Design exterior doors to be sturdy and close fitting, with hinge pins that cannot be removed.

- Equip with thief-resistant locks
- Consider external intrusion alarm system.
    - Connect to central control unit at security station or police station
    - Include procedures for servicing alarm calls
- Design emergency exit doors to open from the inside
    - Unsupervised emergency exit doors can be equipped with delayed locking devices with local alarms
    - If permitted by local fire code, set delay to thirty seconds, rather than the standard fifteen seconds
- Except as emergency exits, do not use collections storage room doors as external exit doors
- Monitor exterior doors left open for public access, deliveries, and staff use.

The primary entrance door for some archival facilities may be internal doors within a larger facility. When possible, work with the building management to provide appropriate security at the primary building entrance and at the entrance/exit archival facility doors.

In many areas, first responders coordinate with local residents, businesses, and institutions to provide a secure key box accessible only to first responders. This box holds the keys necessary to access all spaces in a building in the case of an emergency. Consult with local fire, police, and EMT services to determine if this is the right solution for the archives facility.

5.3.4 - Additional Exterior Architecture and Buildings Operations Features

Aside from windows and doors, there are many openings in the exterior of a building that can allow for unauthorized entry to a building. Access doors for the building's mechanical, water, and electrical systems, or HVAC intakes and outlets are common examples.

- Consider security grills and alarms for any opening in the building's envelope greater than 10 inches in diameter (25 cm)
- Isolate, to the extent possible, collections storage spaces from the networks of ducts and conduits that have a direct outlet at the exterior of the building

5.4 - COLLECTIONS SECURITY

Although primary consideration is given to collections storage rooms, provide similar security to other collections holding areas, including processing and lab areas. In general (for specifics about doors, locks, and alarms, see 5.4.1-5.4.3):

- Design walls and floor construction for the physical security of the collections
- Design mechanical, electrical, and fire safety systems for the physical security of the collections
- Provide doors, locks, and alarms for collections security
- Locate collections storage separate from the public areas of the building
- Do not store collections in corridors or other unsecure areas
- Provide security for temporary storage of collections on the loading dock/receiving area

5.4.1 - Doors to Collections Areas

- Lock and monitor collections storage doors.
- Use windowless hollow metal doors and frames.
    - Can be manufactured to any dimension
    - Can accommodate different security hardware combinations.
    - Match fire rating to wall fire rating.
    - Wood doors present a fire and security risk.
- Hollow metal doors and frames are classified in levels.
    - Standard (level one)
    - Heavy-Duty (level two)
    - Extra Heavy Duty (level three)
    - Maximum-Duty (level four)
        - Tested to a more rigorous standard
        - Have thicker steel in the door and frames
        - Full flush and seamless
        - Higher fire rating
        - Higher rating to resist intruders and severe weather

- All door assemblies should be subject to the following testing as prescribed by the Hollow Metal Manufacturers Association (HMMA):
    - Static load testing
    - Impact testing (soft body and hard body)
    - Vision system impact testing
    - Forced entry attack testing
    - Jam/wall stiffness testing
    - Edge crush testing

5.4.2 - Locks on Doors to Collections Areas

Provide manual or electronic locks depending upon the facility's security requirements, budget, procedures, and other requirements.

5.4.2.1 - Manual locks

- Procure those with a high security rating and interchangeable cores so that they can be re-keyed for new requirements or lost keys
- Use astragals to shield locking mechanisms, particularly on double doors
- Develop procedures for managing manual locks including:
    - Limit the number of keys distributed to staff
    - Maintain careful records of key circulation
        - Facilities may require daily sign-out and return of keys
    - Ensure the return of all keys when staff leaves archives' employment.
        - Lost or unaccounted keys require replacement and sometimes lock re-keying, which is both expensive and time-consuming

5.4.2.1 - Electronic Locks

- Restrict access to staff only
- Types of electronic locks include:
    - Key fobs
    - Keypad combination systems
        - There is a risk that unauthorized people can get the combination
        - Easy to change the combination as needed
    - Access control cards, such as
        - Magnetic swipe cards
        - RFID cards
        - Smart cards (also called chip cards or integrated circuit cards)
        - Unique ID apps on smartphones
    - Biometric locks
- Electronic locks require secure, back-up source of electricity such as an emergency generator, to ensure that the electronic locks do not become unlocked in the event of a power failure
    - If the electricity renders the lock inoperable, develop a plan for bypassing the electronic lock to access the collections areas behind the lock
- The advantage of electronic access systems is their management via a central database
    - Databases automatically record times when entry and egress to designated spaces occurs, thereby creating an access log
    - Lost access cards or a change in staff can be quickly and easily corrected in the system's database

    - Note that in large enterprises in which the archives are a department, electronic access controls are often managed by non-archives staff. Other classes of employees in the enterprise may be granted “all access” to every electronic lock, such as first responders, facilities management, and information technology staff. It is imperative to communicate with staff who manage access controls about limiting access to the archives collections spaces to only staff and essential staff in the enterprise

5.4.3 - Alarms

In addition to external intrusion alarms, internal intrusion alarms to areas where collections may be held are used for archival security. Alarms can be connected to a central monitoring station or the police. Alarm types include:

- Door alarms
    - Activated if the door is forced open, not properly closed, or propped open
- Motion detectors

5.4.4 - Video Surveillance

Surveillance cameras can be installed to monitor areas where collections are held as well as the corridors leading to those spaces.

- Surveillance cameras cannot automatically detect theft
- Surveillance footage is only useful when it is monitored in real time or consulted after a suspected breech of security
- Store camera recordings for a minimum of 30 days or as long as provided by local statutes, regulations, and records schedules
- A backup electricity source is necessary if a surveillance system’s main source of power goes out

5.5 - LOADING DOCK and RECEIVING AREAS

Include the loading dock and receiving room(s) as part of the entire archives' security systems and procedures. This provides a secure environment for receiving archival materials into the building. Security in these areas protects collections from theft and vandalism, as well as fire, weather, and pests.

- Provide dock doors, whether roll-up or swing, with appropriate security
- Provide internal doors with same security as collections storage doors
- Screen materials arriving at loading dock
    - This includes visual inspection at a minimum and may include metal detection and x-ray inspection
- Separate archival materials from other materials entering the facility and move the archival materials to a separate secure receiving area or to specified collections storage rooms
    - Manually inspect all mail and packages received at the facility
- Provide staff surveillance at loading and receiving

Optionally, the loading dock and receiving areas may have:

- Electronic screening of all mail and packages received
- Recorded video surveillance

5.6 - RESEARCH SPACES AND RESEARCHER SECURITY

Research spaces, also known as Reading Rooms, are secure areas used where researchers have direct access to review and study archival materials. They are designed so that collections are protected from theft, vandalism, or damage at all times. Physical security through the design of the space in conjunction with carefully established security policies and procedures work to provide security for the collections. Although designing spaces with a priority on security may be perceived as creating an unwelcoming environment for researchers, that need not be the case. A well-designed space that empowers staff to work with visitors can be both welcoming and secure.

Refer to section 7.11 for the functions and adjacency requirements for research room(s).

5.6.1 - Security for Entry to the Building by Visitors

Before getting to the research space(s), visitors first enter the building and then proceed through the facility to access the research space.

- Provide a dedicated public entrance separated from collections storage rooms, research rooms, processing and lab areas, and shipping/receiving areas
- Provide high security access controls on all public doors that are engaged when the building is not open
- Provide security guard/receptionist(s) to monitor public entrances during public hours
- Provide monitored and recorded video surveillance of public entrances.

Optionally, an archives facility may have:

- An on-site security command center
- An electronic access control system on select exterior entrance doors.
- Electronic locks and access readers on all exterior doors that are operable from the outside
    - Provides the ability to "lock-down" the facility in the event of a crisis outside of the facility
- Electronic access control system, using a single technology on all or select interior doors
- Electronic visitor screening (X-ray, magnetometer) at public entrances
- Emergency generator to supply any security systems with the requisite electricity

5.6.2 - Security for Visitors after Entering the Building

Depending on the size of the archives facility, or if the archives is one department within a larger building, visitors may have to navigate multiple spaces to access the research space(s). Reduce confusion about who has access to which spaces with well-designed spaces and clear policies:

- Visitor control and screening system
    - Examples: sign-in/out log and/or photo ID check
- Employee photo ID's to be worn at all times
- Roving staff or security patrols during public hours
- Electronic access control system on interior doors to non-public spaces

Optionally, facilities may also use:

- Paper stick-on self-expiring visitor passes worn by visitors at all times.
- Photo ID's for long-term vendor and contractors worn at all times when on site.
- Roving security guard patrols 24/7
- Recorded video surveillance system covering all publicly accessible areas.

5.6.3 - Security for Entry to Research Spaces

- Provide access from the public entrance and/or lobby
- Avoid allowing the public to walk through or by collections storage room or other collections holding areas
- Provide researcher access to collections only in the research areas
- Provide researcher registration, also known as sign-in desk, ideally outside the research room(s)
    - May be located in the building lobby or outside the entrance to research room(s)
    - May be located immediately inside the research room
- Provide lockers for researchers' personal belongings outside the research room(s)
- Provide rest rooms outside the research room(s)
- Provide one secure entrance/exit for researchers
    - Check belongings brought in and out of research space
    - Provide a second secure staff-only entrance, if space allows

Optionally, if the archives is located in an unsecure building, a high-profile building, or where there are significant concerns about personnel safety archives may:

- Provide a magnetometer to check for weapons

5.6.4 - Security in Research Space(s): Design/Layout/Procedures

Sightlines for the staff in the research space is one of the most important aspects of archives security.

- Design the room to provide clear supervision of all researchers by staff and/or monitors
    - Eliminate visual barriers when possible, including columns, shelving and furniture

- Provide a monitoring stations, also called the central desk
  - Depending on the size of the space, provide an elevated platform for better views of the research room
- Layout researcher tables so that they can be monitored by staff
  - Require researchers to sit facing the central desk when possible
  - Restrict access to a limited amount of materials to avoid mixing materials or potential of boxes blocking staff's monitoring.
  - Create enough space between tables to allow for the staff to circulate and for carts to travel between or sit beside tables
- Based on the use of the facility, provide a sufficient number of tables to allow researchers appropriate space to review various types of materials.
- Assigning multiple researchers to a table (four at the most) provides an additional deterrent to theft or damage to the materials when space is a consideration.
- Secure windows with locks and alarms
  - Prevent natural light from falling directly on collections
  - Locate windows so that they are visible to the staff from the central desk
- Secure collections after hours
  - Provide a secure hold area or return materials to collections storage after hours
- Surveillance cameras can be installed to monitor research spaces
  - Surveillance cameras cannot automatically detect theft
  - It is only useful when it is monitored in real time or consulted after a suspected breech of security

5.6.5 - Security Considerations for Additional Research and Learning Spaces

Archives may be used for large-group instruction, tours, lectures, and other such programs. Occasionally, there is a separate space for such programming. When there is not such a space, a research room may be employed.

- Considerations regarding a single point of entry/egress, doors, windows, access controls, intrusion detection, and video surveillance for other areas of the archives apply to separate special programming spaces
- Design the room to provide clear supervision of all guests by staff and/or monitors
- If the reading room serves as such a space, ensure that researcher materials can be stored securely in the space while a large group is in the space to maintain an accounting of archives materials

5.7 – EXHIBITS

Exhibit spaces provide archives with a means of sharing select materials, along with historical context, to large audiences who can engage with the information on their own without the aid of staff. Because of the limited staff interaction with exhibit goers, adjust security measures accordingly.

- Locate exhibition spaces near other public access areas with security from theft or vandalism for archival materials on display
- Monitor exhibition areas
    - Recorded monitoring such as surveillance cameras
    - Roving staff monitors
- Lock and alarm exhibit cases
    - Exhibit cases can be locked with keyed mechanisms or security screws
- When the facility is not open, protect exhibit room(s) with intrusion detectors, motion detectors, other appropriate security measures, or a combination of them
- Consider high-quality facsimiles for exhibition

Optionally, archives can secure exhibit spaces:

- Provide locker or coat rooms to store visitor belongings
- For valuable materials or in an open exhibit area, consider using a photoelectric beam

5.8 - BUILDING AUTOMATION SYSTEMS (BAS)

Newer facilities are incorporating building automation systems (BAS) and Physical Security Information Management systems (PSIM). These solutions allow facilities to reduce costs with improved efficiency and improved security.

- A BAS uses interlinked networks of software and hardware to monitor and control a building's mechanical and electrical systems, lighting, security and fire systems.
- The PSIM integrates security applications and devices and controls them through one user interface. PSIM integration enables numerous organizational benefits, including:
    - Greater control
    - Improved situation awareness and management reporting (identifying and tracking events)
    - Improved communications with the staff who are automatically notified of events and with external entities who may need to respond to events, such as first responders or systems vendors.
    - Situational management (standard operating procedures (SOPs) for incidents) and situation reconstruction or debrief (reviewing the steps and actions that were taken during the incident in search of future improvements)
- Consideration for the design and use of BAS and PSIM systems:
    - Access to the system needs to be limited to authorized personnel only
    - The systems are capable of being isolated and controlled independently, preferably from one central control center
    - The need an uninterruptible power source
    - They need to have robust IT security to protect from cyber-attacks
        - A cyber-attack against a BAS could pose a threat if the attack were to manipulate essential building systems, including fire suppression, security, HVAC, and others [See Section 5.10]

5.9 - TYPES OF PHYSICAL SECURITY SYSTEMS

Archives security, which is about empowering staff to effectively protect archival materials, depends on physical security systems including locks, electronic access control systems, perimeter detection systems, interior detection systems, lighting, alarms, and surveillance equipment to. With varying upsides and downsides, there is no single perfect tool, and a combination of tools is likely the best approach for an archives facility. There are a number of variables to consider when determining the best physical security system for a facility, including a risk assessment, facility design, location, and budget.

Some archives facilities, when part of a larger enterprise such as a city government or a higher education institution, may have in-house providers of security systems, such as a locksmith. Archives staff are encouraged to work with the locksmith or other security professionals to ensure the needs of the archives are met and within the possibilities of what the enterprise-wide security systems can provide.

5.9.1 - Locks

Because the majority of entries into a facility occur through doors, provide a quality locking system for both exterior and interior doors. Provide:

- Windowless, hollow metal doors located where an intruder cannot use a broken adjoining window to unlock the door from the inside.
- Inward-facing hinges with pins that cannot be removed.
    - If outward-facing hinges are necessary, fixed-pins that prevent jimmying are imperative.
- High security locks with multiple-pin tumblers, deadlock bolts, interchangeable cores, astragals, and serial numbers.

Table 5-1 LOCKS FOR ARCHIVAL FACILITIES

Locks	Recommended	Recommended with Reservations	Not Recommended
Double Bolt lock	X		
Drop bolt/deadbolt lock	X		
Mortise double cylinder deadbolt lock	X		

Interconnected lock		X	
Mortise or cylinder Deadbolt lock		X	
Spring bolt lock			X
Key-in-the-knob lock			X

5.9.2 - Electronic Access Control Systems

Electronic access control systems control access through a door using a keypad, card, smartphone, or biometric identifier. Considerations include:

- Systems require backup power source to guarantee continuity of security in the event of an electrical outage.
- A combination of an electronic digital lock with an electronic control system (card reader) create an even more secure environment.
    - An electronic digital lock is operated by entering a combination into an integrated keypad
        - Can be keyless or combined with key for additional security
        - This security measure is limited to a single door and it cannot record entries
    - An electronic control system uses an electronic ID reader. Features include:
        - Programmed to limit access by time of day, location, specific IDs
        - Provides auditing features, including logs of entries/egresses
        - Provides remote administration
        - Quick revisions to access system
        - Can be used with:
            - Key fobs
            - Magnetic stripe cards
            - RFID cards
        - Smart cards (also called chip cards or integrated circuit cards)
        - Unique ID apps on smartphones
- Biometric Identification measures the physical characteristics of a person, such as hands or eyes to determine authentication and control access
    - Can be used on single doors or programmed into card-reading access system

5.9.3 - Perimeter Detection Systems

Perimeter detection systems are designed to detect intrusion through doors, windows, skylights, and other apertures in the facility. Most devices are electromechanical and transmit an alarm if the electrical current moving through the system is interrupted.

5.9.3.1 - Detection Systems for Windows

- Foil tape on window panes to protect windows against vandalism
  - Foil tape readily deteriorates, can be easily damaged, and is expensive to install and maintain
- Glass break detectors attach to windows and contain a small frequency sensor that detects breaking glass
  - Effective, but the device and wires are visible at all times
- Audio glass break detectors can be mounted on the wall in a small room with several windows
  - Usually connected to the alarm system and are only armed when the alarm system is activated
- Security screens function like ordinary window screens except that they include tiny interwoven wires that alert the alarm system when the screen is removed or cut
  - Custom and expensive
  - Permit ventilation, when appropriate, without sacrificing security

5.9.3.2 - Detection Systems for Doors

- Magnetic door contact switches consist of electric current running through two contacts, one attached to the door frame and one attached to the door. When the contact is broken, the alarm sounds
  - Reliable, but can be bypassed by using a strong magnet
- Balanced magnetic door contact switch uses a closed magnetic field
  - Difficult to bypass
  - Must be precisely mounted
  - Matched when manufactured so they are not interchangeable
- Door prop alarms sound if the door has been left or propped open longer than a set period of time
- Latch position indicators set off an alarm if the door has not been latched properly

5.9.3.3 - Detection Systems for Walls, Windows, and Doors

- Vibration detectors sense movements in walls, windows, doors, skylights, etc. when an intrusion is attempted

5.9.4 - Interior Detection Systems

Interior detection systems sound an alarm when an intruder is inside a locked facility. Most systems operate by sensing movement in the area. Each system reacts differently and to different situations so designers must determine which system(s) works best for any given area in a facility and the overall security program.

Some systems may trigger nuisance alarms depending on the location of the device and how it is used. For instance, an HVAC system that moves a high volume of air may move vertical blinds in front of an office window; that movement may trigger a motion detector. Minimizing nuisance alarms is not only appreciated by those who respond to them, it ensures that all alarms are taken seriously and met with the appropriate responses.

5.9.4.1 - Mat Switches

Mat switches consist of two pieces of conductive materials that are kept apart by a material barrier. When weight is placed on the mat, the conductive materials touch, completing an electrical circuit and setting off an alarm. These are often located at archival facility entrance doors.

5.9.4.2 - Stress Sensors

Stress sensors work on the same principle as the mat switches and monitor extra weight being placed in an area. They are often placed on load-bearing beams under areas to be monitored, including roofs.

5.9.4.3 - Ultrasonic Devices

Ultrasonic devices send out a balloon-like pattern of high-energy sound waves that are picked up by a receiver. Interruption of the waves sets off the alarm. These waves cannot penetrate walls so their use is restricted to rooms without interior barriers. They can be used in rooms with multiple doors and windows as long as barriers are not present.

5.9.4.4 - Microwave Alarms

Microwave alarms establish an electromagnetic field that triggers an alarm when disturbed by an intruder. The shape of the field can be adjusted to cover a long corridor or an open space. Microwaves can penetrate wood, glass, drywall, and similar materials so placement is crucial to avoid false alarms. Because they can penetrate walls and more, they are easier to hide and monitor areas in other rooms. Problems may arise if the beams penetrate exterior walls and respond to exterior movement such as passing vehicular traffic, resulting in false alarms.

5.9.4.5 - Photoelectric Beams

Photoelectric beams transmit infrared or ultraviolet beams to a receiver. They are particularly effective in long corridors or to restrict access to whole sections of a building. They can also be camouflaged as ordinary electrical outlets as well as small boxes on the wall or on a column.

Often, these are used to protect uncased materials in exhibits, because they can provide a barrier that visitors cannot pass without setting off an alarm.

5.9.4.6 - Infrared Sensors

Passive infrared sensors "examine" an area searching for changes in infrared energy or temperature emitted from objects in the area and set off an alarm when changes occur. These units are sensitive enough to detect changes near an air-conditioner or radiator. Therefore, placement is crucial to avoid interference in their field of "vision." These are often used in reading rooms and large stacks.

5.9.4.7 - Dual Technology Sensors

Dual technology sensors combine the capabilities of ultrasonic devices and passive infrared sensors. Both devices must be activated for an alarm to occur, minimizing false alarms. These can often be used in reading rooms and large stacks.

5.9.5 - Alarms

Security systems rely on two types of alarms: local and silent. Silent alarms are recommended for archival facilities.

- Local alarms set off a loud noise and/or flashing lights when activated. This is designed to cause the intruder to leave the scene and alert the intruder's presence to patrolling police and/or passersby. Such alarms do require immediate police or security response, which likely is not effective for an archives facility.

- Silent alarms are wired directly to a police department, central monitoring location, alarm company, or campus security. In this instance, the intruder has no knowledge that the alarm has been triggered. Assuming that there is a quick response, there is a better chance of apprehending the intruder.

5.9.6 - Lighting

Archival facilities should provide enough exterior and interior lighting to prevent dark spaces where intruders could hide. A well-lighted exterior will deter a potential intruder from spending time trying to break into a facility when the risk of being observed is high. See Section 3 for lighting guidelines.

5.9.7 - Surveillance Equipment

The most common forms of surveillance equipment are closed-circuit television (CCTV) and the cloud-stored video surveillance footage. Surveillance cameras can be installed to monitor the perimeter of the building, exterior doors, the loading dock, stacks, reading room(s), exhibits, public access areas, corridors, and office areas. Cameras can be effective for observing patrons, but they are not infallible in detecting theft in the reading room or other areas of the archives facility. It is difficult for staff to maintain constant TV monitoring, so some archives only use the camera footage when a researcher is suspected of theft or mishandling records. Motion activated cameras can alleviate having to store hours of uneventful footage and the need for very large video storage equipment. Retaining footage for 30 days, or as long as provided by local statutes, regulations, and records schedules, gives archives staff time to return to the footage after a potential theft or vandalism event. A battery backup system or emergency generator ensures the surveillance system will work in the event that the main power source goes out. Because of low lighting conditions in most facilities when staff are not present, the system should work in low light conditions of 2.8 foot candles [30 Lux]. Refer to section 3 for lighting guidelines.

Surveillance technology rapidly evolves and advances in Building Automated Systems and Physical Security Information Management systems will rapidly change how surveillance systems are used in archives facilities. [See Section 5.10 Cyber Security]

5.10 - Cyber Security

Security for archives facilities is not only about protecting physical materials held within the walls, but it is increasingly about protecting born-digital and digitized records as well. Additionally, archives operations—HR and personnel management, documentation of workflows and policies, accessions information, records management communications, building systems management, and more—are part of integrated, and often cloud-based, networks that are susceptible to cyber-attacks.

Because new threats emerge frequently and cyber security is constantly evolving, ensuring that an archives facility is protected from cyber threats is an ongoing endeavor. The Cybersecurity and Infrastructure Security Agency (CISA) in the United States and the Canadian Centre for Cyber Security (Cyber Centre) provide comprehensive resources and guidance for small, medium, and large organizations, including national, state/provincial, and local governments, and academic institutions.

Unfortunately, electronic and IP-enabled (internet protocol) systems for archives facilities are susceptible to all threats common to traditional IT systems. These threats include cyber-attacks such as:

- Viruses and other malware
- Phishing
- Distributed Denial of Service (DDoS)
- Intrusion into servers to alter digital files or to gain unauthorized access to sensitive material including emails
- Intrusion into Building Automated Systems to cause disruptions with the building's operations, which may be used to commit further crimes against an archives facility

Basic steps that will protect archives facilities IT infrastructure include:

- Secure all electronic systems with robust authentication protocols, firewall, and network monitoring, especially those systems that function through the building's IT network
    - Particularly vulnerable systems are those connected to the internet/IP-enabled, including:
        - Building Automated Systems (BAS)
        - Servers storing born-digital files
        - Office computers, which can contain sensitive emails and donor and personnel files
- Secure, with the appropriate doors, locks, surveillance, and intrusion detection systems, any rooms used to store network and IT infrastructure
- Consider requiring the use of a VPN for remote access to the organization's network
- Consider requiring multi-factor authentication

- Consider requiring regular training for staff about cyber threats and how their good cyber hygiene practices can secure the facility and the organization
- For digital preservation, engage a service that uses a network of geographically distributed servers to mitigate corruptions to any single copy of a particular file