# Suggested Practices for Museum Collections Space Security

As adopted by:

The Cultural Properties Council of ASIS International and

The American Alliance of Museums


The Cultural Properties Council of ASIS International has adopted ***Suggested Practices for Museum Collections Space Security***, as described in this document. “Suggested practices” are not best practices, and this document does not attempt to establish best practices. Not all aspects of all recommendations will apply to all museums. But most will apply or can be closely adapted by any museum institution calling itself a museum or gallery. Smaller museums in particular may find it difficult to comply with the recommendations herein. The Council recognizes that museums are so diverse in nature that there will be those for which these Suggested Practices do not apply. While the recommendations as adopted are voluntary, they represent the composite opinion of the leading experts in the field of museum security as being appropriate for most, it not all, institutions. In fact, there will be few exceptions. While they may apply to historic houses or sites, libraries, and other cultural properties, they were not specifically developed for these applications unless they function as “museums.” We are hopeful that these Suggested Practices could be developed for these specific applications in the future. It is also our hope that, in time, the suggested practices will be used by accreditation personnel as guidelines for evaluating the security of an institution.

# Table of Contents

## I. Statement of Purpose

Museums and other cultural properties typically have a large number of vaults, rooms, and areas that are dedicated to the housing and care of the collections. The purpose of these Suggested Practices is to identify the minimum procedural and physical security requirements for those areas. The Suggested Practices are necessary to protect from loss or damage of the museums' collections and loaned collections that are in the museums' custody.

The ***Suggested Practices for Collections Space Security*** outlined in this document are a supplement to the ***Suggested Practices for Museum Security*** as adopted by the Museum Association Security Committee of the American Alliance of Museums and the Cultural Property Council of ASIS International.

The intent of these Suggested Practices is to provide guidance towards risk mitigation while considering the balance between access and handling requirements and best security practices. These Suggested Practices should be put into practice in conjunction with the collections other related policies.

Where applicable, each museum's collecting unit, in conjunction with the security chief, may establish unit-specific requirements and procedures in addition to these Suggested Practices. Solutions outside the published Suggested Practices may be viable if they meet the spirit of the Suggested Practices for protecting the collections.

## II. Applicability

These Suggested Practices apply to all existing museum collection spaces—owned and leased collections storage rooms, buildings, and facilities—httand to new collections spaces as they are constructed or acquired.

For purposes of these Suggested Practices **"collections space"** is defined as:

> An area, owned or leased, enclosed or outdoors, the primary purpose of which is to permanently protect and preserve, through managed environmental and security controls, collections owned by or in the custody of the institution in furtherance of its mission; and may include adjacent areas that provide managed environmental and security controls suitable to accommodate temporary use of collections. This use may

include but is not limited to storage, registration, processing, conservation, study, photography, preparation and packing, and movement.

For purposes of these Suggested Practices. "collection management staff**"** is defined as:

> Any staff (i.e., registrars, curators, conservators, etc.) that require regular access to use and/or manage the safety and security of museums collections.

The practices in this document apply to areas that permanently hold collections, as described in the definition, and other spaces that temporarily house collections for a significant period of the time. Other spaces may be defined as “collections space” based on their assigned function, and the duration and frequency of holding collections. All such cases will be assessed on an individual basis with practical consideration for how and why collections are accessed and used.

All existing collections space should strive to be compliant with applicable minimum suggested practices.

All new or renovated collections space should be planned and designed to be compliant with the policies, procedures, and design best practices identified in this document. Additionally, new or renovated collections space should strive to be compliant with the suggested practices.

Spaces that might contain collections but are nonetheless exempt from meeting these Suggested Practices include public space, exhibition space, and areas generally called “open storage.” For security guidance for these types of spaces reference the *Exhibit Case Construction and Alarming Design http://www.asisonline.org/councils/MLCP.xml.*

These Suggested Practices do not address security of collections in transit.

## III. Risk Levels

The risk to any collection item is the result of a combination of several factors that can vary significantly from item to item.

The mitigation measures appropriate for reducing risk for any particular collection item should also correspond to these factors. The risk mitigation best practices, policies, and procedures identified in this document were developed to apply to collections in four risk categories as shown below. Assignment of collections to these risk categories shall be carried out by unit collections management staff, with assistance from the security chief as necessary.

The primary factor used to assign the appropriate risk category should be the perceived and/or actual value (or significance) of a collections item. Value, and the impact of loss or damage, can be defined in one of several ways including, but not limited to:

- Intrinsic value
- Cultural value
- Research value
- Reputation of the institution
- Mission of the institution
- Use and required access

When determining the appropriate risk categories for collections, staff should consider these various forms of value or significance as they apply to the following risk category definitions:

A. Low Risk

Items are considered to be of such value that the impact of their unauthorized access, removal, theft, or damage would not be significantly detrimental to the image or reputation of the museum. Duplicate or replacement items might fill their void.

B. Medium Risk

Items are considered to be of sufficient value that the impact of their unauthorized access, removal, theft, or damage would be significantly detrimental to the image or reputation of the museum.

In the absence of any risk category designation, the default risk level assignment for any collections would be that of Medium Risk.

C. High Risk

Items are considered to be of sufficient value such that the impact of their unauthorized access, removal, theft, or damage would be highly detrimental to the image or reputation of the institution and could impact the mission of the museum.

D. Very High Risk

Ownership or display of the items is a newsworthy event. Items are considered to be of sufficient value such that the impact of their unauthorized access, removal, theft, or damage would be extremely detrimental to the image or reputation of the institution such that the ability of the institution to receive borrowed collections or gifts may be impacted.

Note: Objects on loan may carry conditions that require a level of protection above that which the museum would normally establish if the item were in its collections.

## IV. Collections Space Access

A. Principles

Although the mission of the museum and its collecting units require that collections are made available for study and educational purposes, physical access to collections space must be balanced against preservation and security concerns. Access to collections space shall be limited to the minimum number of staff whose official duties require frequent and regular access. Staff who does not require such access should not receive access and/or keys to collections space. Additionally, unescorted access should only be granted to employees and staff who have an official institution credential issued on the basis of an appropriate and adjudicated background investigation. This includes affiliated staff such as interns, volunteers, contract staff, visiting researchers, etc. Any employee or affiliated staff that does not have an official institution credential issued on the basis of an appropriate and adjudicated background investigation should be escorted at all times when in collections space.

Each collecting unit should maintain specific procedures regarding access to collections spaces. These specific procedures should be developed for each risk level. In other words, the procedures should identify the types of positions and staff that should receive access to each collections space. Procedures should also consider interests and needs of other collecting units when multiple collecting units reside in a single facility or building. However, at a minimum, unit-specific procedures should adhere to the requirements outlined in this section.

B. Authority

All requests for access to collections space by access card and/or key should be submitted in writing by the requestor and should require signature approval by:

1. Requestor's supervisor
2. Designated Collections Management staff responsible for the management of the collections space
3. Collecting unit Director or Director's delegate
4. Security Chief for the facility or Security Chief's delegate

Collecting units shall keep an access list to each collections space. Access lists are lists of staff authorized to have electronic access, key access, or the authority to deactivate intrusion detection sensors (through coordination with the facility's security control room). Access lists may also be used to identify those collection management staff that should be informed in the event of an emergency that may affect the collection. Collections unit management and the Security Chief shall work to develop the access lists and should maintain the official copies of the access lists. Access lists should be reviewed bi-annually by the Security Chief for the facility (or delegate) and designated Collections Unit management staff.

Electronic access cards and keys for each collections space will be held in a sealed security control key box for emergency access.

C. Electronic Access for Card Readers

Parameters for levels of access are programmed into each access control/electronic security system and define when and which doors/elevators museum credential holders are authorized to access. Access levels, coinciding with facility operations and collections risk levels, are determined by collaboration between the Collections Unit management and the Security Chief.

When a collections space door outfitted with a card reader is opened, the access card holder who opened the door should ensure that there is no unauthorized access behind him/her. Access card holders shall not open collections space doors for unauthorized persons lacking collections space access. Upon request, the Security Chief will provide collections management staff with entry and exit logs (where applicable) for collections spaces.

D. Keyed Access

Many collections spaces do not have electronic card readers installed and access is controlled through keys and locks. If an area is outfitted with an electronic card reader, keys that bypass the electronic lock should not be issued to any staff for regular access.

When card readers are not used and the only lock is a mechanical lock, single doors should be equipped with high security deadbolt locks and double doors should be equipped with high security drop bolt locks. Collections space keys should be kept in Security's control and issued daily as needed to authorized staff. Procedures for collections spaces that have not been outfitted with electronic card readers should be identified in a policy that categorizes (by risk level) who can be issued keys to collections space, the management of such keys, and procedures for emergency access. Collections space keys that are signed out by authorized staff should never leave the facility or be transferred to another person.

The opening of keyed access collections space doors for extended periods or for any purpose other than emergency egress, must be coordinated with the Security Chief prior to opening.The Security Chief should maintain a copy of the access list for each collections space, which should be used to identify staff authorized to coordinate such openings. If prior coordination is not accomplished, and a collections space door is opened, a silent alarm will be sent to the security control room. This will require security staff to respond to the door location. When a collections space door (not outfitted with an electronic card reader) is open for an extended period, a collections management staff person should monitor the open door at all times to ensure that there is no unauthorized access. Security staff may be called to support this monitoring if arranged in advance.

When collection storage is equipped with overhead doors used for movement of collections, the controls for opening the door should be located inside the collection storage room and should be key or card reader operated.

E. Visitor Access

For purposes of these Suggested Practices, any person who does not have an electronic access card and/or authority to sign out keys to the collections space is considered a visitor to the collections space. Visitors may be both individuals with an official museum credential and those without.

1. Temporary Access

Museum collections spaces, reading, or study rooms are accessible to users according to the policies and procedures established by individual Collections Unit. Users are persons having a demonstrable academic, cultural, or artistic interest that requires direct access to the collections consistent with the museum's mission. Unplanned or *ad hoc* access is usually not provided. Collections Units should develop specific procedures for user access based on the nature of their facilities and collections, logistics, and the risks to their collections. At a minimum, all procedures should include:

- Collections are accessible only by advance arrangements with authorized staff within the relevant Collections Unit.
- Users' requests should be specific. Casual browsing and additional impromptu requests should not be accommodated.
- Users who are visiting in collections or records spaces must be accompanied by a staff member with authorized access to those areas.
- Backpacks, briefcases, and most personal items should not be permitted in collections spaces.
- Established collections handling and inventory procedures must be followed by users. Staff should advise users or provide written guidelines for handling procedures and rules for particular use areas.
- The museum reserves the option to restrict access due to resource limitations, security threat level, object availability, intellectual property rights, applicable restrictions, and preservation constraints.

Authorized staff (sponsors) granting access to collections should provide oversight during the collections visit. Sponsors are responsible for ensuring that visitors have checked in with Security and have received a museums visitor ID Badge, know the emergency exit routes, and understand collections handling and use policies and procedures. Sponsors should be responsible for ensuring that visitors exit collections spaces properly.

Visitor Logs: All visitors must sign a visitor log, maintained by the collections management staff, when entering the collections space with their escort/sponsor/authorized staff. All visitors must provide the following information on the visitor log:

- Name (tour groups may be logged in as a group but a participant list should be provided prior to the tour)
- Address
- Dates of visit
- Purpose of visit
- Business or home phone number
- Business or home email
- Collections to be accessed
- Museums sponsor name
- Institutional/tribal/group affiliation if relevant

2. Tours

Tours of collections space for target audiences are an important part of some museum's outreach efforts. Each Collections Unit should have written procedures defining acceptable tour parameters, including:

- Procedures for scheduling tours
- Size limits for tours and number of tour “guides” required based on tour group size and demographic (e.g., tours involving children may require additional supervisory efforts). There should be at least one trained staff person who conducts the tour and at least one other staff person who remains with the tour at all times.
- Safeguards to be taken based on collections risk levels
- How to handle deviations from the tour route (e.g., restroom breaks)
- How to handle emergency situations
- Responsibilities of each staff member assigned to the tour
- Provision of training for tour “guides” in acceptable tour practices

- Acceptable use of photographic, video, and audio equipment in collections spaces (generally not allowed)
- Carrying of bags and parcels into collections spaces (generally not allowed)
- Age restrictions (if any) on tour members
- Appropriate oversight for tours including younger persons, such as requiring the presence of chaperones.

## V. Moving Objects from Collections Spaces

### A. Principles

There are many mission-essential reasons for moving museum collections within a facility or between museums facilities. Tracking and securing collections movements and relocations within and among collections spaces and museum facilities is an essential risk management activity. Generally, these movements can be classified into two main categories:

- Object(s) Movement: When some objects, but not all, from a collection or collections are moved to a transitory or temporary space, for reasons such as exhibition preparation, study, conservation, or space renovation, for a finite period of time.
- Collections Relocation: When an entire collection or the collection contents of a specific space are relocated to another space for an indefinite period of time.

### B. Object(s) Movement

#### 1. Objects Moved Within a Facility

Collecting Units should develop object movement security procedures collaboratively with the Security Chief. These security procedures should address how object(s) will be protected based on risk, value, and the locations and timing of movements, including protocols for collections management staff to give timely notice of movements of large numbers of objects through public spaces within the facility to the Security Chief. This allows the Security Chief to arrange appropriate levels of protection services for the objects. All movement should be documented by collections management staff. Software products exist that may be helpful in tracking this movement.

2. Objects Moved Outside of a Facility

Object movements from museum facilities to any location other than the originating facility shall be documented by collections management. The documentation should include an authorization form that should be reviewed by security prior to collections leaving the facility. If movement of objects from a facility involves loading collections into a vehicle at a museum's loading dock or zone, collections management staff shall give timely notice to the facility Security Chief so that he/she can ensure appropriate security staffing at the designated area.

C. Collections Relocation

1. Planned Relocation

There are many possible reasons that may require the relocation of a portion or all of a collection to a new collections space. Some of the possible activities associated with a planned relocation include, but are not limited to:

- Movement to a space within the same facility
- Movement to a space within a different facility
- New purchased or leased space

A Planned Relocation process requires the coordination of many elements, including the Security Chief, to ensure the new space or site will meet the minimum requirements for security (often based on a formal threat and risk assessment), environment, and safety controls.

*Note: Collecting Units should not, under any circumstances, relocate collections or collection items without coordinating with the Security Chief.*

## VI. Physical Security Measures and Practices

A. Principles

Physical security measures are considered the physical characteristics (equipment, construction methods, or location) of collections space that are used to mitigate the risk to collections located within. These measures are intended to deter, detect, and/or delay unauthorized access to a collections space and allow Security staff to respond in an appropriate manner.

The Collections Space Physical Security Design Criteria, located in Appendix "A" identify by risk level[1] the physical security measures recommended for new or renovated collections spaces. The following measures supplement those identified in Appendix A.

B. Physical Security Measures

1. Electronic Access and Card Readers

All staff access to collections space should be through doors outfitted with an electronic access card reader which provides an audit trail of the user. Although normal key locks and mechanisms may exist on doors outfitted with card readers, they shall not be used, except in an emergency or if the card reader fails.

2. Doors, Openings, and Locking Mechanisms

All doors or other movable openings to collections space must remain closed and locked and all perimeter intrusion alarms on doors or other movable openings will be armed and monitored at all times except when accessed by authorized staff.

If a door is opened without using the card reader, a local audible alarm should sound and a silent alarm will be sent to the local security control room. This will require security staff to respond to the door location and follow security protocol:

If a door outfitted with a card reader is opened for an extended period of time, a local audible alarm will sound and a silent alarm will be sent to the local security control room. This will require security staff to respond to the door location and follow security protocol. The opening of a door outfitted with a card reader for an extended period (e.g., for moving in collections or large equipment) must be coordinated with the security control room prior to opening. The security control room shall maintain a copy of the access list for each collections space that shall be used to identify staff authorized to coordinate such openings. When a collections space door outfitted with a card reader is open, a collections management staff person should monitor the open door at all times to ensure that there is no unauthorized access. Security staff may be called to support this monitoring if arranged in advance.

[1] Refer to Section III

3. Electronic Intrusion Detection

Intrusion detection devices shall be disarmed by authorized staff upon entering the space either by an alarm/disarm panel within the collections space or by coordinating with Security for deactivation upon entering the space. Security will maintain an access list of all staff authorized to enter the space and request deactivation of the intrusion detection. The intrusion detection will be reactivated (by either alarm/disarm panel or by Security) upon departure from the space for extended periods, or at the end of the business day. It is the responsibility of the authorized user to verify with Security that the collections space has been closed and armed.

4. Mechanical, Electrical, and Plumbing Systems

With the exception of fire protection systems, collections spaces should be relatively free of systems that pose a risk of water damage if possible. This may include water pipes running through the room, sinks, or toilet facilities. However, when such systems are unavoidable, or desirable for operations, water detection systems should be installed to provide adequate notification of water leaks or flooding.

Collections space should not contain mechanical, electrical, or other equipment that necessitates access by contractors, building engineers, or others who would not otherwise have authorization to enter secure collections space. If dedicated systems are required for a particular collections space, the systems should be located in adjacent areas with separate access arrangements, but not within the collections space.

5. Separation of Collections (separate space)

Collections management staff should consider separating collections spaces by department or by access requirements. This more readily enables the unit to reduce the frequency of legitimate access to the space and also divides the target assets, making them more difficult to locate and gain access by unauthorized persons.

6. Separation of Collections (within the same space)

Staff should also consider additional separation of collections within a collections space. Small or easily pilferable (or easily concealed) items should be

reasonably separated and secured to both restrict unauthorized access and support inventory practices.

Additionally, if a collection contains relatively few (or physically small) High Risk items, it may be more efficient to store those items in a separate cabinet or safe, within another, lower risk collections space. The cabinet or safe should meet all of the High Risk physical security requirements in this instance.

7. Storage Cabinet Keys and Combinations

If used, storage cabinets and safes should be keyed with unique keys or combinations so that access to an individual cabinet can be given to a specific staff member without providing access to all cabinets or safes. Keys and combinations should be stored in a locked key cabinet under the control of Security. Combinations should be placed inside a small sealed envelope with an identifying number, not a description of the safe and location. A log for key or combination issuance should be kept that is separate from collections space access. Locks for collections cabinets should be of high quality and should be pick resistant.

8. Emergency Egress

Collections spaces should not be located in the direct path of egress for a facility. In other words, emergency egress paths should not be planned to direct staff or visitors through a collections space.

9. Avoid Mixed Usage

Avoid mixing any other functions such as general office space, work areas, or non-collection storage with collections spaces to limit access to collections. The nature of the collections, and their use, may not make this possible in all cases.

## VII. Disaster Management

As part of a unit's Disaster Management Plan, specific procedures shall be developed to mitigate the impact of potential natural or man-made disasters on a collections space. The procedures and plan shall identify the following steps for each type of collection:

- Preparedness measures to protect collections space prior to the occurrence of potential disaster
- Response and notification procedures to protect collections spaces during, or shortly after, the occurrence of a disaster
- Short- and long-term collections spaces recovery procedures after a disaster has passed.

## Appendix A: Collections Space Physical Security Suggested Practices

The following physical security measures are recommended for design and construction/renovation of museum facilities. Each collection storage area will be assigned one or more measures, per category, based on the risk category assignment of the collection. See Table A (below) for the measure assignment based on risk category.

All new or renovated collection storage areas or facilities should be planned in accordance with these minimum Suggested Practices. Existing collection storage facilities should strive to meet this Suggested Practices where and when possible.

- Location (of the collections space)

  Measure 3: This space shall be located in a staff only area.

  Measure 5: This space is a staff only area and shall be internal to the building and not be adjacent to external walls or public areas.

- Walls

  Perimeter protection encompasses the entire space envelope. The delay times shall be calculated based on the threat using unlimited hand tools and limited power and thermal tools. All barrier walls shall extend from floor to ceiling slabs and be constructed in a manner to provide visual evidence of unauthorized penetration. Openings which penetrate a wall (including HVAC ducts) that are larger than 240 sq. cm (37 sq. in) with any dimension being greater than 15.25 cm (6 in), shall be protected with burglar bars to mitigate intrusion. Burglar bars shall be #5 rebar forming a rectangular web that is welded 125 mm (5 in) on center both horizontally and vertically.

  Measure 1: No special measures required.

  Measure 3: Shall be constructed of 16-gauge or greater steel studs spaced 16 inches on center (OC) and gypsum wall board (GWB) with 9-guage expanded metal screwed securely or spot welded every 150 mm (6 in) on the non-secured side of the metal stud behind the GWB.

  Measure 4: Shall meet one of the following:

  i. Be constructed of 16-gauge or greater steel studs spaced 16 inches on center (OC) and gypsum wall board (GWB) with 9-guage expanded metal, screwed securely or spot welded every 150 mm (6 in) to both sides of the studs behind the GWB.

ii. Be constructed of 20 cm (8 in) concrete masonry unit (CMU) with #4 rebar every course and mortar filled.

iii. Meet eight minute forced entry delay.

Measure 5: Shall meet one of the following:

i. Must be constructed of 20 cm (8 in) reinforced concrete with #5 rebar spaced 15 cm (6 in) each way and rebar shall overlap between floor and ceiling pans.

ii. Meet 11 minute forced entry delay.

- Windows

Perimeter glazing and protection encompasses the entire space envelope. The delay times shall be calculated based on the threat using unlimited hand tools and limited power and thermal tools.

Measure 2: All operable perimeter windows within 4 m (18 ft) of exterior ground surface or within 3 m (12 ft) directly or diagonally opposite a window, structure, fire escape, or roof shall be fitted with a positive latch or deadbolt to maintain the opening closed or be permanently closed. A window is considered permanently closed when a non-destructive mechanism has been installed which precludes opening with ordinarily obtainable tools. Where window hinges are on the exterior of the building and the hinge pins are capable of being removed, the hinge pins shall be either fixed in place with a set screw which is inaccessible when the window is closed or welded in place.

Measure 5: No windows allowed in this space.

Measure 6: Glazing must meet the delay factor of the wall measure.

- Door Assembly

Boundary door protection encompasses the entire door assembly (door, hardware, and frame).The delay times shall be calculated based on the threat using unlimited hand tools and limited power and thermal tools.

Measure 3: The door shall be constructed of metal, metal clad, or 44.5 mm (1 ¾ in) solid wood or meet 1 minute forced entry delay.

Measure 4: Shall be a Class 5-V vault door in accordance with Federal Specification AA-D-600D including a day gate extending from floor to ceiling (preventing individuals from crawling under or climbing over them).Open

metal bar day gates are generally recommended over full acrylic gates for HVAC considerations. Day gates must provide free egress from the protected area. The lock mechanism on open metal bar/mesh gates must protect against fishing the inside handle with a metal implement for entry.

Measure 5:The door assembly shall meet the delay factor of the wall measure.

- Door Hardware

  Measure 3: Conventional key & locking mechanisms only.

  Measure 4: A high security combination lock shall be provided. Consult Security for combination lock specifications.

- Electronic Access Control

  Measure 3: Doors shall be provided with electronic access card readers. Locking mechanisms shall incorporate life safety requirements. Entry control features shall be coordinated with the intrusion detection system so authorized entries do not generate alarm conditions.

  Measure 4: Doors shall be provided with electronic access card readers combined with keypads. Entrance shall be granted if an authorized card is presented AND the proper Personal Identity Number (PIN) is entered. Locking mechanisms shall incorporate life safety requirements. Entry control features shall be coordinated with the intrusion detection system so authorized entries do not generate alarm conditions.

  Measure 5: An exit card reader shall be provided inside the protected space to record the departure of individuals within the protected space. An exit made without using the exit reader shall result in a door forced open alarm annunciated at the door and at Security. The electronic access control system will maintain a list of those individuals present at any time within the protected space.

- Intrusion Detection

  Low Risk: Doors and hatches shall be protected with door position switches. If the space has windows, they shall be protected with glass-break sensors. Ducts requiring protection (see “Walls”) shall be protected with duct sensors. All openings shall be protected with motion detection. The protected space shall report as a unique security zone, independent of other detection devices.

Medium Risk: Doors and hatches shall be protected with door position switches. If the space has windows, they shall be protected with glass-break. Ducts requiring protection (see “Walls”) shall be protected with duct sensors. All openings shall be protected with motion detection. Walls shall be protected with vibration sensors or curtain motion detection to detect wall penetrations. The protected space shall report as a unique security zone, independent of other detection devices.

High Risk: Doors and hatches shall be protected with door position switches. Ducts requiring protection (see “Walls”) shall be protected with duct sensors. Walls shall be protected with vibration sensors or curtain motion detection to detect wall penetrations. The space shall be filled with volumetric detection. The protected space shall report as a unique security zone, independent of other detection devices

Very High Risk or Vault: Doors and hatches shall be protected with balanced magnetic switches. Ducts requiring protection (see “Walls”) shall be protected with duct sensors. Walls shall be protected with vibration sensors. The space shall be filled with volumetric detection. The protected space shall report as a unique security zone, independent of other detection devices

Overhead doors under 12 feet in width shall be equipped with a magnetic door contact to detect opening of the door. Overhead doors larger than 12 feet in width shall be equipped with two magnetic contacts, one located at each end of the door.

- Cameras

  Measure 3: This space requires ‘Forensic Detail’ coverage of everything exiting this space via fixed camera.

  Measure 5: This space requires ‘Forensic Detail’ coverage of all alarm points within this space via PTZ camera.

  Measure 6: This space requires ‘General Surveillance Detail’ of at least 75% of the space via fixed or PTZ.

- Video Recording and Storage

  Measure 1: At a minimum, all camera video shall be recorded at 2.5 images-per-second for 24 hours a day, seven days a week and stored for thirty (30) days.

Measure 2: Video motion detection shall be used to increase the recording frame rate from 2.5 images-per-second to fifteen (15) images-per-second.

Measure 3: Video motion detection shall be used to increase the recording frame rate from 2.5 images-per-second to thirty (30) images-per-second.

Measure 4: Alarm actuation or programmed events shall be used to increase the recording frame rate from 2.5 images-per-second to thirty (30) images-per-second.

- Intercommunications

  Measure 1: No intercommunications required.

  Measure 2: This space requires an emergency call station.

  Measure 3: This space requires duress button(s) connected to Security.

TABLE A: Collections Space Physical Security Measures by Risk Category

| | Architecture | | | | | | | | | | Electronic Security | | | | | | | | Intercoms | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Collection Risk | Location | | Walls | | Windows | | Door Assembly | | Door Hardware | | Access Control | | Intrusion | | Cameras | | Video Recording | | Intercoms | |
| | Existing | New | Existing | New | Existing | New | Existing | New | Existing | New | Existing | New | Existing | New | Existing | New | Existing | New | Existing | New |
| Low Risk | 3 | 5 | 1 | 4 | 2 | 5 | 3 | 5 | 3 | 3 | 3 | 3 | See Above | | 3 | 3 | 1,2,4 | 1,2,4 | 1 | 1 |
| Med Risk | 3 | 5 | 3 | 4 | 2 | 5 | 3 | 5 | 3 | 3 | 3 | 3 | See Above | | 3 | 3 | 1,2,4 | 1,2,4 | 1 | 1 |
| High Risk | 3 | 5 | 3 | 4 | 6 | 5 | 5 | 5 | 3 | 3 | 4 | 4 | See Above | | 3,5,6 | 3,5,6 | 1,2,4 | 1,2,4 | 3 | 3 |
| V. High Risk | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 4 | 4,5 | 4,5 | See Above | | 3,5,6 | 3,5,6 | 1,3,4 | 1,3,4 | 2,3 | 2,3 |