

# **Suggested Guidelines For Museum Security**

As Adopted by

The Standing Committee on  
Museum, Library and Cultural Property Protection  
of the  
American Society for Industrial Security

AND

The Museum Association Security Committee  
of the  
American Association of Museums  
(rev 11/2002)

## TABLE OF CONTENTS

1. List of Sub-Committee Members
2. Preface, Method of Revisions, Method for Adoption of Suggested Guidelines
3. Recommended Protection Practices Applicable to All Museums

### Duty to Protect the Collection

#### Foreseeability of Crime

- 3.0 Foreseeability of Crime Against the Collection
- 4.0 Adequacy of Protection of the Collection
- 5.0 Fire Protection
- 6.0 Burglar Alarms and Security Electronics
- 7.0 Key Control and Retrieval
- 8.0 Security Training
- 9.0 Security Guard Qualifications
- 10.0 Internal Security
- 11.0 Access Control
- 12.0 Parcel Control
- 13.0 Staffing
- 14.0 Miscellaneous Recommended Practices

#### Dissent Footnotes

#### Attachment "A"-Suggested Security Officer Qualifications

#### Attachment "B"-Suggested Museum Employee Pre-Employment Screening

*About Revisions: Revisions were approved in 1997 and in 2002 and are included in this version of the Guidelines.*

Museum, Library, and Cultural Properties Committee members at the time of adoption of the initial document.

Robert B. Koverman, Chairman  
Director of Protection Services  
Art Institute of Chicago  
Chicago, Illinois

Steven R. Keller, CPP  
Museum Security Consultant  
Steven R. Keller & Associates, Inc.  
22 Foxfords Chase  
Ormond Beach, Florida 32174

Douglas M. Emery, Vice Chairman  
Director of Security  
McNay Art Museum  
San Antonio, Texas

Stevan P. Layne  
President  
Layne Consultants International  
Dillon, Colorado

James L. Banks  
Deputy Chief of Operations  
National Gallery of Art  
Washington, D.C.

Ernest C. Lipple  
Owner  
Ernest C. Lipple & Associates  
Speedway, Indiana

Thomas H. Bresson  
Chief Security Services Division  
Smithsonian Institution  
Washington, D.C.

Danny L. McDaniel, CPP  
Director Security & Safety  
Colonial Williamsburg Foundation  
Williamsburg, Virginia

Ronald A. Cundiff, CPP  
Manager of Security Services  
Field Museum  
Chicago, Illinois

Michael J. Daly  
Chief Security & Investigations  
Queens Borough Public Library  
Jamaica, New York

Luis A. Palau  
Chief New York Security Operations  
Smithsonian Institution/New York Operations  
Cooper-Hewitt Museum  
New York, New York

Edward G. Dolan, CPP  
Assistant Chief NY Operations  
The Smithsonian Institution  
New York, New York

Thomas P. Prevas, CPP  
Consultant  
General Security Consultants  
West Hartford, Connecticut

Frank L. Duley

Director of Security  
Mount Vernon Ladies Association  
Mount Vernon, Virginia

Barton Blake Rinehart, CPP  
President  
Rinehart Security Inc.  
Alexandria, Virginia

Wilbur C. Faulk  
Director of Security  
The J. Paul Getty Trust  
Santa Monica, California

Erroll G. Southers  
Chief Protective Services  
Los Angeles County Museum of Art  
Los Angeles, California

## Preface

The Museum, Library and Cultural Property Protection Committee, American Society for Industrial Security, has adopted the "Suggested Guidelines in Museum Security" described in this document.

"Suggested Guidelines" are not standards, and this document does not attempt to establish standards. While some NFPA industry standards are recommended, the use of the term standard in no way implies that the museums who do not adopt the recommendations are in any way negligent.

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 Committee recognizes that museums are so diverse in nature that there will be those for which these guidelines 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, if 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" rather than simply architectural sites. We are hopeful that suggested guidelines can be developed for these specific applications in the future. It is also our hope that, in time, the Suggested Guidelines will be used by accreditation personnel as guidelines for evaluating the security of an institution.

The Committee also recognizes that smaller institutions simply will not have the staff necessary to comply with some guidelines. For example, a primary and very important guideline (4.10) indicates that every museum will designate one staff member as Director, Manager or Chief of Security. The Committee recognizes the concept of "functional equivalents". Smaller institutions are not obligated to hire a staff member specifically to serve as Director of Security. But in

adopting the spirit of the guideline, the small institution will designate one responsible person to hold this title and be responsible for these duties in addition to his or her regular duties. Larger museums will consider whether the security responsibilities in the institution are sufficiently time consuming to necessitate the addition of a staff member in this position.

A careful reading of this document will also reveal that the Committee used the words "shall" and "should" to distinguish between those suggested guidelines which are considered critical as compared to those that are highly desirable.

Prior to adoption, this document was circulated to approximately 1000 members of the museum and security communities for review. The single most frequent comment received was that the Suggested Guidelines do not go far enough in establishing an aggressive security program, particularly for larger institutions. There are certainly some more aggressive measures that are appropriate for larger institutions or institutions with high value assets than for smaller less vulnerable institutions. Therefore, these guidelines do not constitute the total protection program for any institution but serve as a basic foundation upon which a protection program appropriate for the specific institution can be developed.

## Revisions

This document is not intended to guide the total protection program for a museum or cultural property. The Committee has undertaken an ongoing project to add to this body of suggested guidelines. This document, therefore, is incomplete as compared with a comprehensive security program. Revisions will be issued as they are prepared. The clearinghouse for the announcement of revisions and additions shall be the Museum, Library and Cultural Property Committee of the American Society for Industrial Security. The most recent revisions were approved by the Committee in 2002 and this document reflects those revisions.

## Acknowledgment

In preparing sections 1.0 and 2.0 of these guidelines, the Committee

drew freely from a document, Protecting Customers From Crime, by Lawrence W. Sherman, Esq., Crime Control Research Corporation, 1063 Thomas Jefferson Street N.W., Washington, D.C. 20007, and acknowledges his contribution.

## Definitions:

Where the following terms, which are commonly found in this document, are used or defined in the body of the text, they shall be consistent with the intent of the meanings herein, but these definitions may be altered by the Committee to fit the individual and specific needs of this document. Such altered definition shall be clear and unambiguous in the context in which it is used.

**American Society for Industrial Security (ASIS):** Refers to the American Society for Industrial Security, 1625 Prince Street, Alexandria, Virginia 22314.

**Authority having jurisdiction:** The office, organization or individual responsible for approving equipment, installation, policies or procedures. This might include, but not be limited to, the local, state or county police, building code enforcement office, fire marshal, etc.

**Crimes Against Strangers:** Refers to crimes committed against employees or visitors to your museum or its grounds by a person or persons who are not known to the victim as compared to those crimes committed by fellow employees against fellow employees, relatives against relatives, visitors against companion visitors, etc.

**Museum:** A place, regardless of its exact name, where the public is invited to view, handle, or study items that have been assembled into collections. These might include art, coins, decorative arts, photographs, curios, antiques, or similar items. Any facility calling itself a museum. Due to the unique nature of historic buildings, they have been excluded from this document's definition of a museum. Where buildings have mixed use of space such as is found in a cultural center, these suggested guidelines apply to the gallery portion of the facility.

**Museum operators:** Refers to the persons, corporations or bodies, governmental or otherwise, which own, operate, maintain or manage museums of any type.

**NFPA:** Refers to the National Fire Protection Association. Refer to NFPA National Fire Codes as indicated. Whenever a suggested guideline contained in this document refers to an NFPA Recommended Practice and that Recommended Practice conflicts with a Code or Standard of the authority having jurisdiction, the code or standard of the authority having jurisdiction shall prevail.

**Object:** Refers to any accessioned or non-accessioned item on display or in storage as part of the collection in the museum. Can include art, artifacts, specimens, etc. Used to describe the broadest range of objects found in various types of museums.

**Security:** The protection of people and assets from various threats and potential threats. Used interchangeably with the word protection which includes fire prevention and protection.

**Search:** Refers to an examination of objects or parcels coming into, while on the premises, or leaving the premises of a museum. Searches are to be conducted under the advice of legal counsel in order to comply with all applicable laws and individual constitutional rights.

**Suggested Guideline:** A suggested guideline is a procedure, practice, or system that is suggested as a minimum step toward providing proper protection in a facility. For purposes of this document, they are common to all museums. Suggested guidelines are only advisory provisions. Use of the word "shall" indicates that the provision will be implemented if the user wishes to comply fully. Use of the word "should" indicates that the user is strongly encouraged to implement the provision but may elect to do otherwise if conditions so require or justify. "Suggested Guidelines" are not "standards".

**UL:** Refers to Underwriters' Laboratories. Refer to UL, standards as indicated.

When security terms are used and are not further defined, refer to Butterworth's Security Dictionary: Terms and Concepts by John I. Fay, 1987, Butterworths Publishers, Stoneham, MA.

## Suggested Guidelines Applicable To All Museums (Revised - 1997)

### 1.0 Duty To Protect the Collection

1.1 It is the duty of all museum operators to take reasonable steps to reduce the risk of a reasonably foreseeable type of loss from occurring to any object in the collection while on the museum property, on loan, or in transit, by the action of unknown third parties, staff or visiting scholars, or through fire, flood or similar natural disaster or other foreseeable forces of people or nature.

1.2 The scope of this duty should not be limited as to the type, size of museum, its ownership by private or governmental bodies, or its collection.

1.3 If an object is worthy of being accessioned into a museum collection or borrowed for display as a museum object, or when it is worthy of having public or private funds spent for its maintenance, display, preservation or conservation, it is worth protecting to the extent described in this document.

1.4 It is reasonable for museum managers to foresee "normal" losses typical to museum collections and facilities, including losses due to vandalism, accidental damage, theft, extortion or ransom, fire, or disaster, and these protection matters shall be addressed in protection policies adopted by each institution.

### 2.0 Foreseeability of Crime

2.1 It is reasonable to foresee "normal" crimes committed against invitees' persons by strangers to them, if there have been any crimes against strangers within a one-mile radius of the premises in question, or minor crimes suggesting a problem with maintenance of order on the premises within at least two years.

2.2 In order to determine whether crimes by strangers against invitees are reasonably foreseeable, museum operators should take affirmative steps to keep informed of local criminal activity, including regularly requesting the police department to advise the museum operator whether there have been any stranger-to-stranger crimes against persons within a one-mile radius of the premises.

2.3 It is not generally reasonable to expect a museum operator to foresee crimes against invitees to their premises if local police cannot or do not provide local crime information.

2.4 It is reasonable to foresee crimes committed by premises employees against invitees, if the employee previously committed any act of violence on the premises, or if the employee is known to have committed acts of violence elsewhere under similar circumstances.

2.5 It is the responsibility of museum operators to maintain a reporting system to log crimes and serious incidents occurring on the premises involving employees, invitees, their property or museum property. Where the reporting system evidences a trend or pattern of serious incidents, corrective action to preclude recurrence shall be taken and documented.

2.6 It is the responsibility of museum operators to take steps to ensure that employees whom they hire do not pose a risk to staff, invitees, museum properties, or the collection.

### 3.0 Foreseeability of Crime Against the Collection

3.1 It shall be assumed that risks against the collection, including vandalism, accidental damage, theft, extortion or ransom, fire, or disaster, are foreseeable to any collection.

3.2 It is the responsibility of museum operators to report losses truthfully, such as those cited above in 3.1, so that the full extent of crimes against collections can be understood and foreseen by other museum operators.

3.3 Museum operators should subscribe to publications or services which report museum-related losses of the type pertinent to their institution. "IFAR Reports" and the FBI crime bulletins report on thefts of art.

3.4 When objects are placed in transit, it is reasonable to assume that they are under greater risk than they are while secured in the museum. Therefore, the Security Manager shall be notified and consulted prior to the object leaving the museum so that adequate security can be provided during transit.

#### 4.0 Adequacy of Protection of the Collection

4.1 The term "protection" is best thought of as an overall program in effect in a museum to safeguard its collection. "Protection" is a concept which integrates "security" and "fire prevention" with disaster and strategic planning and post-theft recovery.

4.2 Every museum must view protection of the collection from potential risks as one of the important objectives of the institution.

4.3 It is recognized that the display of valuable and important objects, such as in a museum setting, often results in a risk which might not be acceptable for other valuable or important commodities. Therefore, protective steps shall be taken to safeguard the collection from risks and to overcome the inherent risks of display and exhibition.

4.4. Every museum shall have a written protection program and written policies and procedures. Where a specific issue is addressed in these Guidelines, a formal policy must be included in the policy manual that addresses the implementation of that Guideline.

4.5 The goals and objectives of the security function shall be documented and defined. It is appropriate for this to be done in the Employee Handbook and signed by the chief executive officer.

4.6 There shall be a written manual to be followed by the protection officer and defining how he is to react to various situations. It shall be endorsed by the museum's chief executive officer.

4.7 Every museum shall assign ultimate responsibility for its protection program to one individual at the management level.

4.8 The protection program shall be funded as an identifiable line item in the budget so its adequacy in relation to other expenditures can be judged by management and accreditation bodies.

4.9 Every museum shall have individuals present at all times who perform a security function. While it is most desirable and appropriate to have on-site protection personnel full-time, in some cases it may be acceptable or necessary to assign gallery and perimeter security duties to properly trained and screened non-security personnel such as receptionists, docents, gallery attendants, or other museum staff. The decision to use non-security personnel shall depend upon the risk involved, the value or importance of the collection, its vulnerability, display methods, and other factors. (See "Dissent" note 1.)

4.10 One person shall be designated as being in charge of and responsible for security. When the museum is of the size to warrant a protection department, the individual in charge shall be titled as Director, Manager or Chief of Protection and shall be above the level of "Chief Guard." When there is no protection department, the individual to whom ultimate protection responsibility has been assigned (4.7) shall be designated in this role.

4.11 The security manager shall report to a high-ranking official in the organization. While it is not necessary for the Security Manager to report directly to the Chief Executive Officer, he or she must have direct access to that level of management and must be invited to use that access as desired. Ideally, the person responsible for security should report directly to a Deputy Director or higher. Smaller institutions without a formal rank structure shall observe the spirit of this guideline.

4.12 There shall be management support for the security program and there shall be one person at the highest management levels at the rank of Deputy Director or higher who is responsible for security and for the success of the program. The assignment of this person as the person

ultimately responsible for the security program shall be stated in an official written policy or position description.

4.13 There shall be a commitment by museum management that the security program is applicable to everyone and that no one, because of his or her position, rank, title, status or for any other reason, is exempt from compliance with the policies and rules that are designed to protect the collection, visitors, and staff. The Committee has identified the tendency of museums to make exceptions to the security rules for trustees, volunteers, VIP's, donors, key staff, board members, members of affiliated groups, and others as a primary reason for the breakdown of security operational procedures and discipline.

4.14 It is inappropriate and inadvisable for management to cave in to criticisms about security rules or their impact. It is irrelevant that the security program is not popular with employees. The Committee has identified the tendency of museums to avoid sound security procedures because of their lack of popularity with staff or their impact on the operational status quo, as a serious problem to be avoided.

4.15 There shall be communication between the security management and the remainder of museum management. Inclusion of the Security Manager in department head level staff meetings is important to the success of the program.

## 5.0 Fire Protection

5.1 Every museum shall be protected by a modern, electronic, early warning fire detection system which complies with NFPA standards and is listed as approved by Underwriters' Laboratories (UL) or a similarly acceptable testing laboratory.

5.2 All fire detection systems shall be annunciated within the facility both visually and audibly. Signals shall be clear, distinguishable from other signals and easily understood by all occupants of the building including people who are disabled.

5.3 Fire detection systems shall, in addition to local annunciation, be monitored at a second location that is manned 24 hours per day, 7 days per week. These monitoring stations may be municipal police, fire, or emergency dispatch centers or they may be commercial central monitoring stations. Commercial central monitoring stations should be UL-approved and periodically inspected and recertified by UL. These systems should comply with NFPA 71 and NFPA 72.

5.4 When a decision is made to use the services of an uncertified central station, the decision shall not be economic in nature and shall be with the advice of competent authority. An uncertified central station shall not be utilized without, as a minimum, an on-site inspection of its facilities by a person capable of assessing the ability of the uncertified central station to operate appropriately and with reasonable competence and security.

5.5 All museums should have fire suppression systems. At a minimum there shall be portable fire extinguishers placed in strategic locations throughout the building in accordance with NFPA 10. Fire extinguishers shall be checked daily and inspected for proper maintenance monthly.

5.6 Automatic fire suppression systems should be used. These systems may consist of water sprinkler systems, halogenated extinguishing systems (after a careful evaluation of the environmental impact of such systems) or other automatic suppression systems. The most reliable system is the water sprinkler system; while a wet pipe system is the best, a cross-zoned, dry pipe, pre-action systems can be used. It is best to install suppression systems throughout the museum, but at a minimum, sprinkler systems should be installed in all non-public areas of the buildings, especially offices, shops and other work spaces, kitchens, storage rooms, loading docks, heating plants, wash and rest rooms, etc. Installation of these systems shall conform to one of the following applicable standards:

- 3 NFPA-I 3 Standard for Installation of Sprinkler Systems
- 3 NFPA-12 Carbon Dioxide Extinguishing Systems
- 3 NFPA-12A Halon 1302 Fire Extinguishing Systems

- 3 NFPA-12B Halon 1211 Fire Extinguishing Systems
- 3 NFPA-17 Dry Chemical Extinguishing Systems
- 3 NFPA-I IA Medium and High Expansion Foam Systems

5.7 It is recommended that only water sprinklers and Halon 1301 systems be used. Halon is not intended for use in public spaces where exiting during a discharge may cause loss of suppression gas. Halon is best suited for enclosed spaces such as art or object storage. Museum management will consider the environmental impact of systems using halogenated gas before selecting it. They should also consider the possible worldwide ban on the use of certain extinguishing agents. (See "Dissent" Note 2.)

5.8 Where hose systems or standpipes are used, they shall be installed in accordance with NFPA-14.

5.9 All fire suppression systems shall be inspected on a regular basis for operability. Water systems shall be inspected in accordance with NFPA 13A, Recommended Practice for the Inspection, Testing and Maintenance of Sprinkler Systems. Other systems shall be inspected, tested and maintained in accordance with their applicable NFPA standard and the manufacturer's recommendations.

5.10 Fire detection systems shall be inspected regularly in accordance with their applicable NFPA standards or prevailing local codes, if more stringent. The building shall be examined frequently to verify that it meets local and state fire codes and good practices.

5.11 Fire exits shall be installed throughout the facility to facilitate egress from the building in emergency situations. Proper signs shall indicate where it is impossible for people with disabilities to exit. Where local jurisdictions permit, the exit doors should be locked in accordance with NFPA-101, Life Safety Code. At no time when the building is occupied shall exits be otherwise obstructed.

5.12 HVAC Systems should be installed in accordance with NFPA-90A, Standard for the Installation of Air Conditioning and Ventilating Systems. There should be automatic fire dampers and fan shutoffs in all

ducts to prevent the spread of fire and smoke throughout the building which would further damage collections in areas not directly affected by the fire.

5.13 All museums shall publish and implement an evacuation plan involving employees and visitors which addresses the need for additional security during evacuations. A minimum of one full-scale drill per year shall be implemented and all staff shall be required to fully participate. The needs of the disabled shall be addressed.

5.14 NFPA Standard 911, "Recommended Practices for the Protection of Museum Collections" shall be adopted for museums, and NFPA 910, "Recommended Practices for the Protection of Libraries and Library Collections," shall be adopted for libraries and portions of museums used as libraries. Where 910 and 911 conflict due to mixed use of space in a facility, seek the guidance of the NFPA or a qualified protection consultant for advice.

5.15 Personnel from the fire department serving the museum shall be invited into the facility on a regular basis to tour and to establish a tactical plan for fire response.

## 6.0 Burglar Alarms and Security Electronics

6.1 All museums shall have intrusion detection and signaling systems. These systems shall be monitored 24 hours per day, 7 days per week. Alarm annunciation shall be both audible and visual. There shall be an annunciation on the local premises and a back-up annunciation at a commercial central station, or, where jurisdiction permits, at the police or emergency dispatch station.

6.2 Museums with highly-trained and adequately-equipped full-time professional security staffs may establish a proprietary central station within a secure portion of their building but, as a minimum, a UL-listed panic device shall link the control room to an outside central station. The level of line supervision for the communications link shall meet or exceed "Standard Line Security" as defined by UL Standard 287, Central Station Alarm Service.

6.3 All exterior doors shall have magnetic switches to alert the monitoring station when there is an unauthorized opening of the door. Contacts shall, when practical, be concealed in the door. When surface-mounted, they shall be on the protected side of the door. Exceptions may be made when contacts are not practical due to potential damage to historic fabric. In such cases, motion detection shall be provided.

6.4 All exterior windows which open shall have magnetic switches or other sensing devices which alert the monitor when a window is opened or left open. When windows are locked or otherwise secured, this provision may be waived.

6.5 All doors which have glass, and all windows, shall have glass break detecting devices that alarm when the glass is broken, or interior volumetric motion detection to sense intrusion.

6.6 At strategic places throughout the building there should be motion detection to detect the unauthorized movement of people through the building or area, and to detect persons staying behind after hours.

6.7 Collection storage rooms will remain locked at all times and shall be alarmed when not occupied. As a minimum there shall be magnetic switches on the doors. Other sensors shall be installed in the room or on the interior walls of the room to detect forced entry through the walls. Ducts and other possible points of entry necessitate motion detection or equal protection.

6.8 The use of programmable access control systems employing digital keypads or cards or biometric readers on collection storage is encouraged.

6.9 Safes and vaults which contain collections, money, or other valuables should be alarmed or shall be located inside secure storage rooms or rooms which are protected by motion detection.

6.10 Exhibition halls shall have intrusion detection systems to signal an intrusion into the hall if it is not open. Where possible, exhibition halls should have lockable doors that are alarmed when the hall is

closed.

6.11 Selected items on exhibit or in cases may need the additional protection of detection devices that are active 24 hours per day. The determination of which items should be alarmed will depend on value, replaceability, sensitivity to controversy (such as political and social considerations), ease of sale by a thief, vulnerability to damage by vandalism or unintentional curiosity such as visitor touching. Items which can be secreted on the person, under a coat, or in a briefcase, purse or box should be displayed in exhibit cases. The following items shall always be displayed in exhibit cases or permanently affixed to the building so that they cannot be removed: items made of precious metals, gems, firearms, edged weapons, currency, coins, jewelry and stamps.

6.12 Selected paintings hung in exhibitions should be alarmed so that they signal the monitoring station and/or the local guard when they are touched or moved. The device should alarm if the painting is removed from the wall or when it is lightly touched either by the hand or by a knife blade or similar tool. The criteria for selecting which paintings to alarm is the responsibility of the museum director after consultation with the person ultimately responsible for security or a competent security advisor. Criteria for deciding which paintings require alarms is similar to the criteria outlined in 6.11.

6.13 Whenever there is an alarm, there should be a response to the alarm by a trained guard or other person with security training. Alarms shall not be ignored nor shall assumptions be made about their origin. Building alarm systems which are designed or configured so as to permit a person in a proprietary or off-site central station to make decisions as to whether or not an alarm requires full response, shall be carefully considered before being installed. Such systems include, but are not limited to, those systems in which the monitoring guard is permitted to listen in to activity in the museum or observe television monitors, and then decide if a response is necessary. While UL approved systems employing this technology are not in themselves unacceptable, the Committee expresses its serious concern that any system that allows a guard or system operator to make decisions regarding response to the site of the alarm are not always appropriate for use in museums.

6.14 Whenever a museum conducts its exhibition by tours only, such as in historical houses, there must be some means for the docents or tour guides to surreptitiously summon help if they notice items missing or if a visitor becomes unruly or otherwise disobeys the rules, or if an emergency occurs.

6.15 There should be police call buttons at cash registers which permit the calling of the police in case of a hold-up. These devices should be installed in such a way that the clerk may activate the alarm without the knowledge of the criminal. The alarm shall be silent locally, though it may annunciate in a proprietary or off-site control room.

6.16 Whenever practical, alarm systems should be hard-wired. They should be electrically supervised so that attempts to cut the wires, damage or remove the detection device, ground the system or short out the circuit will send a signal to the monitoring station.

6.17 Where hard-wired burglar alarm systems are not practical, wireless systems can be used. These systems also shall be supervised so that, at a minimum, they will 1) signal when their batteries become discharged below a minimum power level and 2) require the control panel to poll the detectors at least once per hour, or more frequently as UL standards require.

6.18 There shall be a regular inspection program for all alarm systems. Each system should be activated to ensure that it is working, motion detectors shall be walk-tested to ensure that they are still covering the area they originally intended to cover, etc. Testing shall be continuous and ongoing.

6.19 Alarm systems shall be fully supervised against tampering. The system shall signal tampering not only between the control and the multiplexer or data-gathering panel but also between the multiplexer or data-gathering panel and the detector. Tampering with signaling devices on the circuit connecting them to controls also shall be detected.

6.20 Alarm systems shall be capable of operating during a power failure for a minimum of 24 hours on batteries, power supplies, generators or by other means, and longer if local conditions require.

6.21 For buildings which are unoccupied for part of the time and where it is necessary to shunt the alarms upon arrival for the day, a duress signal capability shall be provided. This shall be accomplished by way of a keypad with a confidential, silent duress code or by similar means.

6.22 The method of electronic communications between the premises alarm system and the remote monitoring facility shall comply with Underwriters Laboratories Standard 827, Central Station Alarm Service, and meet the equipment listing requirements for at least the "Standard Line Security" level of protection service against compromise. A compromise is the disconnection of the protected premises from the connecting line or communications channel in a manner that does not cause a signal at the central station and therefore allows entry into the protected premises without initiating a signal at the Central Station or blocks the transmission of an emergency signal, request for assistance, or burglar alarm signal.

6.22.1 Where the communications link is less than UL "Standard Line Security," it is considered to be unprotected, and the decision to utilize an unprotected communications link shall be made with the full knowledge of the highest levels of museum management.

6.22.2 The decision to use a communications link that is not protected against compromise shall not be based solely on technological considerations.

6.22.3 The decision to use a communications link that is not protected against compromise shall not be based solely on economic considerations, such as the extensive costs of providing secure communications due to the distance from the central station, without a full understanding of the risks of such unprotected communications. The Guidelines recognize that some cultural properties, like log cabins and Indian ruins, may be remotely located, far from central stations or in areas without phone service, making a secure communications link economically impossible. It is a more difficult

decision for larger, less remote institutions to operate with an unprotected communications link solely due to the cost of the service.

6.22.4 When an institution's highest authority makes a decision to operate with an unprotected communications link to the central station, it must be after consultation with the museum's insurer or an independent, non-product-affiliated protection consultant who shall offer alternate acceptable means and technological alternatives. A report must be provided which clearly defines the reason for not providing a protected communications link. The report must define the alarm system in sufficient detail to enable a lending individual or institution, insurer or other party with an interest in the security of the institution to evaluate the level of security that exists. This enables lenders and insurers to evaluate the risks and request other appropriate safeguards such as extra guard protection during loans or special exhibits, etc.

6.23 There shall be a program to regularly inspect alarm systems to ensure their continued effectiveness. Museums are in a state of change. Hanging walls, cases and other changes to interior spaces reduce burglar and fire alarm effectiveness by blocking detector views, etc. After each renovation, installation or redecoration, alarm and detection systems shall be inspected for obstructions and other related problems, and corrections shall be made immediately. Every effort shall be made to prevent such problems by involving the security manager in construction, installation or redecoration plans.

6.24 Museums shall make every reasonable effort to comply with at least Underwriters Laboratories "Extent of Protection Level 4 Coverage" protection with regard to their burglar alarm systems. Individuals advising the institution on adequacy of interior protection must be fully conversant on museum security and the requirements of a changing museum environment as well as electronic security as it relates to museums.

6.25 Museum burglar alarm systems shall avoid integration with the institution's computer network where possible. Systems such as but not limited to ethernet-based point monitoring, access control systems and in some cases digital video shall use their own dedicated network(s). Although most proprietary networks appear secure, threat from public

hacking or virus attack still exists and has successfully occurred in museums. There are situations where museum security systems must share the building's computer network due to infrastructure and or extraordinary budget limitations. In this event steps must be taken to insure the integrity and survivability of critical security functions. In all cases, direct involvement of the museum's professional information technology department head is mandated and the information technology professional charged with the responsibility for assuring the security of the security system. Practical application of "VLAN", segmented firewalls, data encryption, limited trusts, and other advanced technologies shall be carefully considered.

6.26 Museum burglar alarm systems shall not be connected to any phone line on a continuous basis except for the purpose of transmitting an alarm signal off site. It shall not be used for internet access and it shall not be constantly connected via modem to facilitate diagnostics. When diagnostics or programming are required, the service personnel shall call in and request that the modem be temporarily connected to facilitate the diagnostics. The connection shall be made after proper verification. The museum shall establish a formal written policy that defines the steps to be taken to verify the caller's identity and need for modem connection and assures that the phone line is disconnected immediately following the procedure, service or programming. This document recognizes the need for "dial up mode" connections between physically separated buildings. When dial up mode is necessary and a direct connection is not practical, steps shall be taken to prevent and detect hacking including but not limited to firewall protection.

6.27 Museums with PC based point monitoring and access control systems shall have a written policy that forbids any guard or other employee from using the computer for any purpose other than its intended purpose, specifically the policy shall prohibit insertion of any disk or other media into the computer or downloading any file from the internet. When the system is used for departmental administration it shall be equipped with virus software that automatically checks for viruses on a scheduled basis and whenever media is inserted. The museum shall have a written policy that requires that virus definitions be updated on a regular basis, no less

frequently than every 14 days. Responsibility for this task shall be fixed with one individual.

6.28 When a museum is part of another corporate or institutional entity such as a university and the museum's card access system is shared with the other entity, control of the programming of the museum's access cards shall be under the control of the museum and not delegated to others. When this is not acceptable, it is mandatory that museum collection rooms with accessioned items be equipped with high security dead bolt locks that are not on the other entity's keyway or under the control of others. It is not acceptable for both the key cards and the mechanical keys to be on a system beyond the direct control of the museum. This document recognizes that in a university or corporate environment it is not always possible to carefully enough control who is assigned to program card keys. In universities, student employees often are assigned to this task even when officially campus police are officially responsible. This may be acceptable for campus buildings in general but not for high security storage in museums.

6.29 When a museum is part of another corporate or institutional entity such as a university and services are provided to the museum by the other entity such as engineering services by campus facilities personnel, rapid or unrestricted access to all parts of the museum may be required by those providing the services. When this condition occurs and service providers must have keys, the service provider shall not also have the ability to turn off alarms. Any non-emergency access to collection storage or other high security areas such as but not limited to galleries under installation shall be obtained after coordinating the visit with security. Emergency access requiring rapid entry by the service provider can occur using the assigned key but only when an alarm is activated. Rapid entry keys to collection storage deadbolt locks can be provided using alarmed armored rapid entry key boxes such as a Knox box or equally secure product. Every effort should be made to not provide service providers from other entities codes to the alarm system.

6.30 When a museum is part of another corporate or institutional entity and the other entity mandates a "one card fits all" policy, meaning that they require that the same employee or student ID card serve multiple functions

such as card access campus wide or serve as a student debit card, and that all card readers on campus use the same card key, every effort should be made to prevent this policy from reducing security of the collection. When practical a card reader with PIN pad should be used on collection storage doors.

## 7.0 Key Control and Retrieval

7.1 All museums shall practice sound key control and retrieval and shall have a written policy.

7.2 Only those persons needing a key or needing access to a key shall be given that access.

7.3 There shall be good-quality, pick-resistant locks on all exterior doors and hatches, whether they are at or below ground or one or more stories above ground or on the roof. Windows should be locked with a pin or a lock that cannot be opened easily by breaking a small pane of glass. Cam locks should not be the only devices used to secure windows. Doors with windows in them or along side of them should be locked with double cylinder locks. Exceptions may be made for protection of historic fabric.

7.4 Doors to collection storage areas and other areas where collections might be stored temporarily shall be locked with a good-quality deadbolt lock or equal.

7.5 All keys that are issued shall be signed for on a register. Keying systems shall be of the type that are difficult to reproduce except by a bonded locksmith.

7.6 A proprietary or regionally proprietary keyway shall be used when possible. As a minimum, exterior doors, doors to high value storage, and doors to other high security areas shall be secured with high security locks of the type which use key blanks which are not available through local locksmiths, hardware stores, or other suppliers without, at least, a signature authorization.

7.7 Key blanks shall be carefully controlled.

7.8 Locks shall be re-keyed whenever a key cannot be accounted for or keys are known to have been lost or stolen.

7.9 There shall be a key retrieval system to ensure that all keys are turned in when an employee leaves the museum's employ.

7.10 Keys shall be stored in a secure space or container where they cannot be removed without authorization.

7.11 One person shall be responsible for key control, issuance and retrieval.

7.12 Key control and retrieval shall be under the control of the security department when possible.

7.13 Cam locks, except high security types, shall not be used for display cases.

7.14 Bitting codes and un-coded room numbers shall not be stamped or embossed on keys.

7.15 Paintings should be firmly fixed to the wall so that they cannot be easily removed. The use of security screws and brackets, hangers with locking devices, or other similar methods that require a knowledge of the attachment system and time to remove them should be used

## .8.0 Security Training

8.1 Every museum shall have a training program for its security personnel or personnel who serve in a security capacity, or shall obtain training for them from outside agencies. Museums with security supervisory staff shall provide special training to the supervisory staff to ensure that they are capable of performing their duties.

8.2 Larger regional museums of notable reputation and small museums with valuable or important collections shall adopt a more extensive formal

training curriculum for its personnel than might be required in smaller institutions. Nothing in this suggested guideline prohibits the use of a more comprehensive training program. The extent and type of training to be provided shall depend upon the individual circumstances of the museum, its setting, collection, and other factors including local, state or national licensing laws.

8.3 Smaller institutions with lower value, replaceable, or less important assets shall provide a formal training program for its security personnel or those who perform a security function. As a minimum, training should include one full day of classroom instruction prior to reporting to duties, and sufficient on-job training under the direction of a competent and experienced supervisory employee to ensure the proper performance of the security duties.

8.4 The museum shall provide an ongoing training program to keep protection personnel in tune with museum operations and needs and to expand security, fire, safety and first aid and related skills.

8.5 There shall be a comprehensive training manual outlining all basic and advanced topics covered in regular protection staff training.

8.6 Records shall be maintained showing the training materials presented, the date, time, instructor, and employees trained.

## 9.0 Security Guard Qualifications

9.1 All persons assigned to serve in a security capacity shall be physically, mentally and otherwise fit to perform in that capacity. (See attached for guidelines.) Where armed security officers are used, they shall comply with all state and local requirements.

9.2 All persons who serve in a security capacity for a museum shall be subjected to a background check consisting of the elements described in the attached document: Museum Employee Pre-Employment Screening Guidelines.

9.3 The Committee recognizes the need, in some cases, for armed security in the museum. These situations might include museums in high crime areas or with highly vulnerable assets. Armed officers are not normally required or advisable in most institutions. Museum operators shall provide extensive training and pre-employment screening to all armed personnel, and they are encouraged to seek the advice and counsel of their legal advisor, their protection consultant, and local police agency before arming officers or developing a training curriculum for them. Officers who are armed shall be held to a higher standard of physical and mental fitness than unarmed officers.

## 10.0 Internal Security

10.1 All museums shall have a written policy outlining their internal or personnel security program.

10.2 All people working in the museum, including volunteers, shall complete a full job application and shall authorize the museum to conduct a background check as appropriate.

10.3 All employees, volunteers, and docents hired for work in the museum shall be subject to a comprehensive reference check and review of their personnel application as a condition of employment.

10.4 All employees who have access to the collection, master keys, collection storage or exhibit space keys, large amounts of cash, or other valuable assets or materials shall be subject to a background check as a prerequisite for employment.

10.5 Background checks for employees requiring a "clearance" shall include, at a minimum, those elements outlined in the attached document: Museum Employee Pre-Employment Screening Guidelines.

## 11.0 Access Control

11.1 All museums shall adopt a policy on access control which regulates access of all persons including: all staff at all levels, contractors, visitors, scholars and others. This policy will define who may enter the

facility, and, as appropriate, high security areas of the facility, and the hours of the day and days of the week they may enter or be denied entry.

11.2 Access to non-public portions of the museum should be limited to those persons needing access to carry out their duties.

11.3 Employees shall not be permitted to work or to remain in the museum after hours if doing so results in diminished security. This might occur if their presence prevents the alarm system from being activated and when supplementary guard presence cannot be provided in unprotected spaces.

11.4 Visitors to non-public portions of a museum should sign in and be announced.

11.5 Access to collection storage shall be limited to staff with a need to visit storage. Scholars and students who require access to the collection materials shall be accompanied at all times by qualified professional or protection staff personnel.

11.6 Tours, members of the public, and the press shall not normally be permitted in storage areas. Educational tours or classes in storage, when undertaken, shall be accompanied by security or security trained personnel on a ratio of at least one security officer for each 10 visitors, plus appropriate curatorial staff. The Committee recognizes the widespread practice of permitting tours in collection storage areas and has expressed its opinion that these tours, while sometimes educationally desirable, have a significant, negative impact on security. Picture taking, including photos by members of the press, are not advisable in collection storage. (See "Dissent Note" 3.)

11.7 Employees and administrative visitors shall be required to enter and leave the museum via designated entrances, controlled by security personnel.

11.8 Members of the public, contractors and others shall be required to enter and leave via entrances under the control of security personnel. All

entrances and exits to and from the museum through which objects may be removed shall be protected by locks, alarms, and/or guards.

11.9 Access to storage and other areas with high value assets shall be controlled by appropriate means such as, but not limited to, locks, alarms, and/or guards.

11.10 All visitors to non-public areas and all contractors shall be issued an ID card which they shall be required to wear on an outer garment at all times when in the building. The card shall be color-coded and numbered so that the identity of the visitor can be easily ascertained by comparing the number with the visitor sign-in log.

11.11 In any museum where the total number of staff members, including volunteers, docents, and unpaid personnel of any category, exceeds 30 people, a photo ID card shall be worn on an outer garment at all times when in the non-public portions of the building, or in the public portions of the building or grounds after hours. All persons shall display their ID card to the security officer when entering the building.

11.12 Photo ID cards shall be no smaller than 2 inches by 3 1/4 inches in size and shall be laminated or otherwise secured to make forgery or tampering unlikely. The card shall include the photo, name, and number of the employee, the name of the institution, date of expiration and other data that management deems appropriate.

## 12.0 Parcel Control

12.1 All museums should control the flow of property in and out of the premises.

12.2 All parcels larger than 11 inches by 15 inches in either dimension shall be prohibited from entry into the museum except by approval of security personnel.

12.3 All parcels larger than the above shall be subject to search by protection officers upon leaving the museum.

12.4 A parcel pass system shall be used to control property entering or leaving the institution.

12.5 All collection materials removed from the building shall be documented through both the Protection Dept. and the Registrar. A counter signature shall be required for any pass or receipt authorizing the removal of material from the collection.

### 13.0 Staffing

13.1 All museum security personnel shall be assigned full-time to their security duties when guarding and shall not also be assigned to sell tickets, perform cleaning duties, give lectures, guide tours, etc.

13.2 Security staff levels, once established, shall remain constant and shall not be diminished by breaks or absences. Sufficient relief personnel shall be provided.

13.3 Protection supervisory personnel and the security manager shall not be assigned to stand post or conduct non-supervisory patrols. All museums shall recognize that supervisory and managerial duties are full-time functions and that they are necessary to the success of the program.

13.4 Security personnel shall be adequately supervised by well-trained supervisors. Guards cannot supervise themselves no matter how small the institution. It shall be recognized that, without first-line supervision, a security program is doomed to failure. Supervisors shall not normally be assigned to stand post, perform non-supervisory patrols, provide guard reliefs, or perform other duties more properly assigned to non-supervisory personnel. There shall be no more than ten guards to one security supervisor with seven guards to one supervisor being the optimum ratio.

13.5 All museums containing high value assets or collections which are of great importance shall be staffed by trained security personnel 24 hours per day, seven days per week including holidays. Security staffing shall not be diminished for holidays. (See "Dissent" Note 4.)

13.6 When the building is to be unoccupied after hours, a thorough fire and security patrol will be conducted prior to closing and immediately after opening.

13.7 Protection staff shifts shall overlap as required so as to ensure full security on the site during shift change times. It is recommended that Protection staff attend a roll call training session of approximately 30 minutes prior to starting their shift. This program should include announcements of importance to protection staff.

13.8 Security personnel may be proprietary (employed by the institution) or contract (employed by a guard agency). Museums shall recognize that, no matter how well trained are the guards who are provided by a contract agency, specific training pertinent to museum security is required. The use of contract guards does not relieve the museum of responsibility for providing or specifying proper and adequate training and supervision or verifying the background and suitability for employment of the contract employee in the cultural institution environment.

#### 14.0 Collection Storage Room Security

14.1 The term "Collection Storage Room" is a general term that refers to any room within a museum that contains accessioned items not on display such as but not limited to traditional storage rooms, the holding area for art at Receiving, climatization rooms, fumigation rooms, the photo studio, mount making rooms, conservation labs, packing and crating areas, the Registrar's work room, clean rooms, laboratories, etc. "Primary Collection Storage Rooms" refers specifically to the high concentration, more traditional room or vault used for storage but not for other purposes. "Storage/Study Rooms" refers to a room used to store accessioned items but also used as an office, research workstation, or public or semi-public viewing or study of the collection.

14.2 Accessioned items shall not be left in collection storage rooms of any type unless they are under the immediate control of someone responsible for their security such as the employee working with or processing them, or they are secured physically or electronically.

14.3 Collection storage rooms shall be physically secure. Deficiencies in their perimeters shall be compensated for by electronic security. It shall not be possible to climb over a wall either due to the low wall height or by climbing over a suspended ceiling into the space. Walls shall be built to the slab above. Perimeter walls should be masonry when practical.

14.4 Collection storage room doors should be at least hollow metal and where wooden doors are used the doors shall be solid core of sufficient strength to accommodate the hardware required. Collection storage door hinges shall be on the protected side of the door (interior) or shall be equipped with hardware or devices that prevent the removal of the hinge pin and removal of the door. Primary Collection Storage Room doors shall be windowless. Any door to any collection storage room with glass shall be equipped with UL listed, burglar resistant glass or window film, with window film rated for small missile impact being the most desirable method of protecting the glass. Exterior windows to collection storage, where they exist, shall be secured by grills or burglar resistant film or burglar resistant glazing.

14.5 Collection storage rooms shall be windowless except for conservation labs and storage/study rooms which may have windows or skylights if proper safeguards are provided as compensation although windows or skylights into any collection storage facility are highly undesirable and are not recommended. This document recognizes the need for natural light in the study and conservation of some accessioned items.

14.6 Where windows or skylights are present in collection storage rooms, appropriate and effective early warning glass break detection must be provided. Impact sensors on the glass is the most desirable means with acoustic detection properly selected for the type of glass an acceptable but less desirable alternative due to the changing nature of some storage rooms where acoustic characteristics may be altered by movement of items in storage. Where collection storage rooms have windows, items shall not be stored or shelved near the glass where a smash and grab theft may occur before effective response can occur. Window's shall be securely blocked and equipped with alarms when collections are stored near interior or exterior windows.

14.7 Collection storage rooms shall be relatively free of mechanical and plumbing systems that pose a risk of water damage. Water detection shall be used when such a risk exists due to the presence of pipes.

14.8 All exterior penetrations to the collection storage room shall be protected by alarms. This includes but is not limited to detection of glass breakage, opening of doors, and penetration via skylights.

14.9 In addition to perimeter protection, collection storage rooms shall also be protected by volumetric motion detection that meets or exceeds UL Extent of Protection Level 2. Care shall be taken to over design the motion detection system so that shelving or large objects added to the room do not block or diminish detection. Motion detection shall also detect against penetration of the space via ducts.

14.10 Collection storage rooms with double doors shall be equipped with a high security drop bolt lock and those with single leaf doors shall be equipped with high security deadbolt locks. When the museum lacks a building wide restricted or proprietary keyway, systems such as but not limited to Medeco restricted locks shall be used to assure key control. Where card or biometric readers are used, a high security mechanical lock is also required. Electric locks are no substitute for a high security mechanical lock.

14.11 Collection storage rooms should be equipped with card or biometric access control devices.

14.12 Electric locks on collection storage doors shall be self locking, fail secure electric locks or strikes and hardware on the interior of the room shall permit staff inside to turn the knob or lever and exit without being locked in. Magnetic locks should not be used on collection storage rooms doors under normal circumstances although this document recognizes the need to use them on some retrofits and certain specialty doors. Local fire codes shall prevail on issues involving fail safe and fail secure locks.

14.13 It shall not be possible to break collection storage room window glass, reach in, and open a door either by turning the thumb turn or

activating the request to exit device.

14.14 Collection storage should be segmented by department or type of material stored. This more readily enables the museum to limit access to specific collections by curatorial department or specific need to use that collection and reduces unnecessary access to the space.

14.15 Small, pilferable, high risk or especially valuable items like jewelry, precious metals, etc. shall be compartmented within the collection storage room in safes or other secure lockable containers.

14.16 Some collections in some museums use museum quality or other storage lockers or cabinets. These are especially useful to security by placing collections out of ready reach of persons who may have access to the room but may not need access to a large number of items. This includes escorted contractors, interns, patrolling guards, or other support staff. Cabinets shall be keyed with unique keys so that access to an individual cabinet can be given to a specific person but access to all cabinets is not also necessary. Keys to storage cabinets shall be stored in a locked key cabinet under the control of senior staff. It shall not be possible for a person who is authorized to be in collection storage but not to have access to cabinet stored collections to enter the cabinet without supervision. Locks for collection cabinets shall be of high quality and shall be pick resistant.

14.17 Collection storage rooms shall be equipped with fire extinguishers of the type approved by the institution's conservator AND the person responsible for security. In any case, the extinguisher must be of the type suitable for controlling a fire in the environment.

14.18 Primary Collection Storage rooms shall not be used as work rooms. Primary Storage Rooms, and Storage/Study Rooms, photo labs, and similar areas where collections are stored but work also occurs, shall not accommodate heat producing appliances such as coffee makers. Coffee makers and other heat producing appliances shall be located outside the fire separation from the collection and in an area regularly patrolled by Guards. Conservation and related labs where collections are held over night but where heat producing appliances are used as a regular

part of the conservation, mount making or other process shall be carefully patrolled by Guards to assure that appliances are safe. Written procedures shall be in effect for staff in those areas to make the appliances safe and for Guards to verify during patrols that they are off.

14.19 Use of sprinklers in collection storage will be a well studied decision involving the person responsible for security, a fire protection engineer with experience in suppression technology, and curatorial or conservation staff. Where Halon or other pressurized, gas-based suppression is used, items shall be stored in a manner that precludes them from being damaged by the violent discharge of the gas in a fire condition.

14.20 Tours should not occur in collection storage. Where educational tours are necessary, the museum shall have in effect a written policy defining the safeguards to be taken and the responsibility of each person assigned to the tour. The policy shall limit the size of the tour to no more than 25 maximum for large rooms and fewer for smaller rooms or rooms with smaller or more valuable items. Tours shall not be conducted in rooms where small, pilferable or highly valuable or important items are not compartmented and stored in secure containers. There shall be at least one person who actually conducts the tour and at least one representative of the security department who remains with the tour at all times. The policy shall address issues like allowing members of the tour or class to leave to go to the restroom without an escort and what to do if someone becomes ill and needs to be escorted out of the room. Further, the policy shall prohibit the use of cameras in collection storage where security equipment or procedures might be photographed. Parcels carried by members of a tour shall not be permitted in collection storage.

14.21 The museum shall address the issue of guard patrol access to collection storage areas in a written policy. When electronics are deemed adequate to protect Primary Collection Storage areas, it may not be necessary for guards to actually enter the collection storage room except to check alarms. When practical, entry into collection storage by Guards shall be a two person assignment. Work areas with heat producing appliances must be checked on fire patrols.

14.22 Collection storage rooms shall not contain mechanical, electrical or

other equipment that necessitates access by contractors, building engineers or others who do not normally have access to collection storage. When access is necessary, these individuals, as other individuals not normally given collection storage access, shall be escorted.

14.23 Key, card or biometric access to collection storage shall be on a "must have" basis. Collection storage rooms shall not be on the building master or grand master key. Access shall be granted only to those needing access as part of their job. Interns, volunteers, adjuncts, and other non-employees shall not be given unescorted access. Scholars shall not be left unattended in collection storage to do research.

14.24 This document recognizes that existing museums may have difficulty complying with some of the above collection storage requirements and that they shall make a good faith effort to comply. New museums, however, shall be so designed and constructed to meet the above requirements.

## 15.0 Miscellaneous Suggested Guidelines

15.1 All museums shall adopt and publish or post a formal list of Rules of Decorum which outline to the public the rules of the museum.

15.2 All museums shall adopt a formal list of protection-related rules for employees, docents, volunteers and others who work in the institution. The rules, which can be in the form of a manual for employees, shall include a statement requiring all personnel to refrain from theft or other dishonest acts and observe standards of ethics in their business and personal lives.

15.3 The security program in a museum shall apply to everyone. Once a policy is established regarding access or parcel control or other measures of accountability, no one, including the museum director, trustees, donors, etc., shall be exempt. No one shall be excluded from rules or safeguards due to rank, education, job function, etc.

15.4 The museum director, trustees, donors and professional staff must recognize the importance of their compliance with all of the rules in a

manner which reinforces the need for and support of security.

15.5 All museums shall undergo a periodic audit of their security and fire protection programs, and an inspection of their alarm systems, by an outside, neutral, non-product-affiliated museum protection consultant or protection professional on loan from another institution. If the latter is used, he or she shall be neutral and shall not be closely associated with the museum's management or protection personnel.

15.6 There shall be an active emergency plan which enables protection personnel to contact off-duty, on-call professional staff members to respond to the museum in an emergency. This program shall be administered by the security manager.

15.7 All museums shall prepare a disaster plan dealing with foreseeable disasters. The plan shall include, but not be limited to, the development of secure off-site storage for collections.

15.8 Smoking shall be prohibited or greatly limited in the museum.

15.9 Coffee pots and heat-producing appliances shall be prohibited in storage and other areas where they cannot easily be monitored. They shall never be timer-activated or timer-controlled.

15.10 The Protection Manager shall be consulted prior to all movement of collection materials of significant value or importance outside the facility.

15.11 The Protection Manager shall complete all pertinent protection-related portions of all loan forms for objects coming in or going out of the building and shall be promptly advised of all security requirements of any contracts for loans or exhibitions.

15.12 The Protection Manager must be encouraged to develop his or her skills by participating in activities sponsored by ASIS, AAM, the National Museum Security Conference--Smithsonian Institution, or similar museum and security-oriented training and development opportunities. Efforts to this end should be funded to the extent that similar skill enhancement programs are funded for other professional staff members in

the museum.

#### DISSENT FOOTNOTES:

1. While the Committee felt that it was acceptable to use non-security people to perform the security function in smaller institutions, most agreed to this provision as an economic reality. But the aspect of this provision that caused the most comment was the statement that persons who perform the security function should be present "at all times" (See Note 4).

2. The Committee recognizes the physical and economic impossibility of retrofitting some facilities with fire suppression. They also gave extensive consideration to the public comment by museum administrators that water sprinklers are unsafe and inappropriate in a museum. The Committee members felt that sprinkler technology had advanced to the point that water-based sprinklers are, in themselves, less of a risk that a fire would be in a building which lacks sprinklers. Some Committee members felt strongly that water based sprinklers pose an insignificant risk. The Committee also advises museums to strongly consider the environmental impact of halogenated gas systems on the atmosphere.

3. No other Guideline drew more response from the museum administrators who reviewed this document than this provision. Security professionals almost universally agreed with this Guideline and endorsed it. General administrators in museums such as business managers who are responsible for security, and registration professionals also generally agreed. Museum directors and curators were loud in their dissent. The Committee is aware that tours of storage are important to the museum's educational mission and is important to fund raising efforts. But the Committee feels strongly that this type of tour poses a threat to security. For that reason, the Committee did not recommend against tours as they originally felt they should do but instead recommended that security staffing be provided as noted so that tours can be conducted with a reduced risk to the collection.

4. Many museum administrators, and one prominent security professional, felt that it is unrealistic that smaller museums provide 24 hour guard

presence. The Committee stood firm in its conviction that having a person on-site is better than not having a person on-site, even when modern electronics are used for protection. There is no substitute for a good security and fire patrol being conducted periodically. The Committee recognizes that this recommendation will be an economic hardship on many institutions, particularly many small, remote sites. The Committee requests that the museum administrators make decisions regarding 24 hour staffing on a non-economic basis when possible, and when making "hard" decisions that are economic in nature, adequate security staffing shall be given equal or greater importance to other staffing needs, as appropriate.

5. There was considerable comment by non-security persons who reviewed this document, that every effort be made to avoid discrimination against the handicapped. The Committee was sensitive to this and agrees. One Committee member recalled a museum that hired a man with one arm for a midnight shift guard position. The man could not carry both a flashlight and a radio at the same time. Another museum hired a man for a night security position who could not respond to a fire or emergency as he was not ambulatory, then made him night supervisor. The Committee cautions that while it is necessary to provide equal opportunity to the physically handicapped, there are operational concerns that the Personnel Administrator may not be fully aware of. And, when someone is placed in a job he or she cannot perform adequately in, and lives or irreplaceable assets are endangered, the matter is serious. The Committee endorses the use of physically handicapped individuals in dispatch, reception/fixed post, or similar positions when appropriate. It noted the large volume of letters regarding discrimination against physically handicapped persons and finds the points well taken. The Committee advises museums to make employment opportunities for disabled persons but to consider the impact this may have on security. One Committee member indicated that the frequent use of persons who may not be physically able to meet the stringent demands of security work results from the fact that many institutions make no demands on guards, expect little of them, and assume that there is no real need for security. As these Guidelines begin to change perceptions of the museum security function, museums must make certain that their guards are appropriate in every way for the tasks they face.

6. A common note of dissent from several of those who commented, including a museum director and a government museum security expert, was that the Guidelines impose an impossible economic burden on small museums. The Committee saw its role as one of "calling it like it is," since small museums are more often victimized than large museums and carry an equal responsibility to their collections and to their guardianship role as do large museums. Many small museums have extraordinary collections and some contain such important collections as the historical records of entire counties or regions.

## ATTACHMENT "A" - SECURITY OFFICER QUALIFICATIONS

The following qualifications are presented as a guide only. While every effort should be made to recruit security officers who meet the qualifications provided, museums must be aware of the various local, federal and state laws which may limit their ability to utilize all of these guidelines. Discuss this matter with your attorney.

Qualification/Level of Importance (Mandatory, Desirable, As Appropriate)

### Physical Capability

Able to walk a patrol 8 hours a day Mandatory

Hold a heavy door open for minutes at a time Mandatory

Place a person at least 100 pounds in a wheelchair Desirable

Climb steep stairs or a ladder Mandatory

20/20 vision (or corrected to 20/40 with glasses) Desirable/Mandatory if armed.

Hear normal conversation (prosthetic acceptable) Mandatory

Bend, stoop or work with hands above shoulder level Mandatory

Talk intelligently over a telephone or walkie-talkie and be understood by other members of the force Mandatory

No amputations, deformities or disabilities that would prevent satisfactory performance of duties (See "Dissent" Note 5, page 15)  
Mandatory

Present a neat, clean non-threatening appearance Mandatory

Lift and operate safely 50 pound fire extinguisher    Mandatory

Lift a small child (50 pounds) and carry in a rescue    Mandatory

#### Mental/Educational Capability

High school diploma or equivalent    Mandatory

Read and understand written material in language of the security force  
Mandatory

No history or presence of any significant psychiatric disorder    Mandatory  
Emotionally stable    Mandatory

#### Other Capabilities

No criminal conviction record indicating moral turpitude    Mandatory

No history of violent acts that would indicate the candidate would harm  
a visitor or employee    Mandatory

No history of child abuse/sexual abuse    Mandatory

Valid Driver's License/safe record    Desirable (Mandatory if driving is  
required)

CPR qualified    Desirable

First Aid Qualified    Desirable

Local or State Guard License or Certificate    Desirable

Pre-employment polygraph where permitted or pencil and paper test  
Desirable

Physical examination by physician    Desirable

Drug test    Desirable

At least 18 years of age      Mandatory

## ATTACHMENT "B"-MUSEUM EMPLOYEE PRE-EMPLOYMENT SCREENING GUIDELINES

The following guidelines apply, in principal, to all museums. It is recommended that individual museums consult their legal counsel prior to implementation of these guidelines as laws vary between various countries, states, and local entities. For purposes of this section, "employee" also refers to volunteers who serve in the capacity of an employee as well as to members of affiliated groups, boards, etc. which have access to the building or the collection on a level equal to that of employees.

For purposes of determining the depth of the background investigation to be performed, museum employees should be divided into three basic categories. The extent of the background check for any given employee may vary with the level of access the employee has to 1) the collection, and 2) other valuable or important assets, and 3) the level of contact that the employee has with the public.

### Levels of Vulnerability

Level 1: Employees with little or no access to the collection including those with no access to the galleries alone or during non-public hours. This might include the gardeners who work outside the building, move freely in the office spaces, but do not have access in the galleries to any greater degree than the general public.

Level 2: General Administrative Employees with "typical" access to the museum building during public and office hours, and non-employees in a similar capacity. They may move through the galleries unattended before public hours or in the early evening before offices close. They do not have access to storage. They do not handle collection materials or valuables. They do not have important keys. They do not have after hour access. They are not assigned in a public contact role that might place a member of the public in jeopardy.

Level 3: Employees with a level of access that poses a higher potential risk, including all employees of the security department, all employees with access to collection storage, those with permission to handle the collection as part of their jobs, such as but not limited to preparators, installers, curators, interns, the registrar and registration staff, the conservators, etc. Level 3 also includes employees with building master keys, exterior building keys, collection storage keys or programming capability on the facility alarm system. Level 3 also includes all cash handling employees, accounting and purchasing department employees, mail room employees, employees who work the loading dock or shipping and receiving, or employees who work with visitor-owned property such as coat room attendants. This category also includes employees or volunteers who work with visitors who might be harmed by the employee in any foreseeable way, especially those working with children.

The job title is not important in determining the level of background check required. It is the level of vulnerability that should determine the amount of time, effort and resources expended to protect the museum facility, its assets and visitors. Smaller museums with few employees may well subject every employee to the Level 3 background check. Larger museums with many employees may find it necessary to adhere to the guidelines more strictly.

### Reasonable Background Investigation for Each Level of Vulnerability

For ALL museum employee applicants, including volunteers, prior to acceptance:

1. All shall complete a formal written job application which contains a release form and permission to conduct a background investigation.
2. All shall be interviewed in person by a responsible interviewer at the professional level.
3. All shall provide several personal and, as appropriate, professional references. These references shall be contacted, and questions regarding the character and integrity of the applicant shall be asked.

4. References shall be verified. The person doing the background investigation shall make sure that the reference is indeed who he or she says they are and not an accomplice of the applicant. Verification might be made by looking the reference up in the phone book and verifying that the number provided by the applicant is correct and that the person being called is not simply posing as the reference.

5. A responsible employee shall verify all information provided on the application form. This shall include accounting for all periods of employment for the past five years, and all gaps between employment, to ensure that the applicant is not hiding incarceration, hospitalization, termination or other relevant conditions.

6. Verification of pertinent license data. Example: An employee requiring a guard certification by a city or state shall be subject to a verification as to that license. An employee with a responsibility for driving a vehicle shall be subject to a thorough check as to his suitability for such a task including inquiry of any extent to determine if the applicant has any health problem, including drug or alcohol abuse history, that might prevent the safe operation of the vehicle.

7. Verify educational background where it is relevant to the job.

For Level 1 Employees:

1. Those elements that apply to everyone.

For Level 2 Employees:

1. Those elements that apply to everyone plus;

2. A criminal conviction history check for a period of no less than five years prior to the date of application, or as far back as is legal in the jurisdiction. This check shall be conducted for all areas where the applicant is likely to have committed a crime, such as in his home city, county, state, etc., as well as in the county in which the museum is located.

3. Make contact with references at previous places of employment for at least the past five years.

For Level 3 Employees:

1. Those elements that apply to everyone plus,
2. A criminal conviction history check for a period of no less than five years prior to the date of application or as far back as is legal in the jurisdiction.
3. A consumer credit check to determine the applicant's credit background, reveal data about his or her character, suggest a potential motive for theft, and provide investigative leads such as the identification of discrepancies regarding prior employment, places of residence, etc.
4. A civil records check to reveal civil actions that may be an appropriate concern.
5. Develop a minimum of three references not provided by the applicant, and obtain from them a reference on the applicant.
6. Verify the educational background of the applicant
7. Obtain a reference from all previous employers in the past 10 years. Question the reference carefully, being aware of the fact that the reference will not always provide straight forward information and that you will have to ask specific questions to bring out the negative information.
8. Photograph the employee and obtain a set of properly inked fingerprints. It is not necessary to submit the prints for review by a law enforcement agency. Retain the prints for future use in the employee's file. Typical use would be to identify the employee's real identity should he or she commit a crime while working under an assumed name.

## Optional Steps That Are Encouraged

1. Where legal, state of the art, validated, pencil and paper personality profile tests are generally considered to be an effective and fair way of determining with some degree of accuracy an applicant's attitude toward honesty, drug use and similar matters.
2. A physical examination, including a drug use test, is encouraged, where legal, but only where properly administered.
3. A Worker's Compensation check, where legal, may be effective in identifying applicants who have left previous employers after committing insurance fraud.

## For Manager of Security Positions

The Manager of Security is a "Level 3" employee, but museums are encouraged to hire a professional "full-field" type investigation where the above information is gathered by a skilled private investigator and analyzed by the investigator, the museum's security consultant, local police officials, or others with experience in the detection of deception and conducting complete background investigations.

## Exemptions

No employee is exempt from the requirement to prepare a formal job application. If a resume is submitted, a job application will also be prepared and submitted for inclusion in the employees file. All applications will contain a release form authorizing the museum to conduct the appropriate level of background check.

No employee is exempt from the appropriate level of background check. Museums shall resist the widespread practice of exempting well known scholars, management level employees, curatorial employees, or others with high rank, reputation or standing from the process.

## Use of Information

All information shall be gathered and maintained in a confidential manner. Museums shall refrain from gathering, and shall refuse to record, report or store information that is irrelevant to the business of determining the ability of the applicant or employee in gaining the necessary security clearance. Such information shall include, but shall not be limited to, information pertaining to the employee or applicant's religion, political convictions including criminal record for civil disobedience not indicating moral turpitude, sexual preference, or similarly irrelevant data. Information that is developed shall become part of an employee's confidential personnel file and shall be maintained in the most confidential manner, when practical, sealed in an envelope within the file so that it is available for future reference, but not readily available to those in the personnel management or administrative capacity without a need to know.

This document does not attempt to define what elements of an applicant's or employee's background render him unsuitable for a position. It is recognized that individuals "reform" and that certain civil information such as a bad credit history or a criminal history involving civil disobedience, while indicating potential risk, do not necessarily indicate dishonesty. It shall be the duty of the security manager, or person responsible for security, to report the facts pertaining to an applicant's or employee's background to the museum's Director through the Personnel Administrator, to decide, with the advice of the security manager, whether the employee or applicant is suitable. It is generally felt that individuals with felony records within the recent past or individuals with arrests for use of any drug or narcotic, should be denied a clearance for work in Level 2 and 3 positions. Exceptions shall be made on a case by case basis and responsibility for such decisions rests with the Museum Director. The role of the Security Manager is that of advocate for the best possible security, and he or she should not be expected to unilaterally, and without the advice and authority of the Director, make exceptions or relax security clearance rules or criteria.

There is no clear-cut criteria for being denied a clearance. It is best that the museum define its criteria, then make exceptions judiciously, recognizing the facts pertaining to the individual involved. The background history of the individual shall not be the sole criteria for

denying employment or promotion but shall be one important factor.

Consult your attorney in developing a policy. This document is a guideline that may or may not be legally acceptable in your jurisdiction.