

Security Recommendations for Houses of Worship

Case made for security for Houses of Worship

2006 Gunman shoots five people at synagogue in Seattle, Washington.

2006 Maryland church robbed during New Year service.

2006 Gunman Kills 4 People at Baton Rouge Church

2005 Multiple Churches are burned in the South.

2004 Church Security Guard shot and Killed in Los Angeles Church Parking Lot.

2004 Gunman kills self inside L.A. Cathedral.

2004 Man drives Bulldozer into Church.

2002 Pastor stabbed while assisting a homeless man.

2001 A New York man tried to handcuff himself to a Roman Catholic Archbishop during New Year Mass.

1999 Forth Worth, Texas – Gunman opens fire at Texas prayer service. 8 people dead.

1999 Arson attacks in three Sacramento area synagogues.

Recommended Practices

Security recommendations for Houses of Worship are intended to assist religious organizations in developing awareness and security for incidents that may occur during their official functions. The recommendations are not regulations or guidelines and should not be construed as such. Hence, they are not binding and are designed to assist organizations in providing useful and learned practices.

Further, some practices for particular functions may be developed later as situations change in the religious environment.

Definitions

Throughout this publication, several terms may be used that may provide the same meaning. They are:

Houses of Worship: Religious institutions of all faiths and denominations may include Mosques, Churches, Synagogues, Sanctuaries, Temples, etc.

Security Force: Security Officer, Security Guard, or Security Ministry.

Community Police Officer (CPO): Local law enforcement officers acting as liaisons between police departments and areas they protect.

Special Events: Conference, seminars, and special missions and Worship services.

Security Plan

Every organization should have a well written security plan that protects against known and expected hazards. The fundamental goal of a security plan is to protect people, facility, and assets.

1. Conduct a risk assessment of the facility and organizational operations. For assistance in conducting a risk assessment, see ASIS' General Security Risk Assessment Guideline at www.asisonline.org/guidelines/guidelines.htm.
2. Provide a written security plan to all responsible for the security function.
3. Review the security plan annually and update according if changes are warranted.
4. Include local law enforcement into the security plan and coordinate for emergency response to the facility or situations.
 - Many law enforcement agencies have designated Community Protection Officers (CPO) to service Church venues.
5. Address personal protection for the religious leader and his or her family within the security plan.
6. Consult legal counsel before implementation of any security plan.

Intelligence

Federal, State and Local resources must be used to determine "HATE" crime activity in the area.

1. Monitor known hate groups in the area. Local police task forces are available to report graffiti and other hate crime activity.
2. Routinely perform internet searches of groups and activity in your local area and across the United States.
3. Ask the youth of the congregation to discuss hate crime activity in the schools and community. Discuss this activity with local law enforcement.

Physical Security

Physical security refers to the tangible objects put in place to protect people and property. Such systems include fences, walls, locks, lighting, surveillance cameras, alarms, and security personnel.

Outer Perimeter

1. Wrought iron fences are aesthetically pleasing and provide physical protection.
2. Fencing assists in controlling pedestrian and vehicular traffic.
3. Lighting should be provided around all outer perimeter fencing and within all parking areas.
4. Strategically place lighting equipment to assist security personnel and the security function.
5. Close circuit television (CCTV) situated on the outer perimeter looking inwards provide surveillance of facility property.
 - Maintain digital video recorder (DVR) for CCTV system at an offsite location to protect against damage arson may cause to the main facility.

*It should be noted that when surveillance images are recorded and stored at a site other than the Organization's facility, there should be firm agreements with any party involved in the capturing recording and storage to recognize that the religious Organization will maintain control and confidentiality of such recordings.

6. Install signage on perimeter structures warning potential trespassers.

Building Perimeter

1. Concrete decorative post situated 4-6 feet from building exterior may keep vehicles from causing structural building damage.
2. CCTV situated on the outer building overseeing parking areas provides deterrence to the criminal element.
3. Provide alarm system for all doors and windows.
4. Test all alarm systems periodically.
5. Work with maintenance personnel to ensure proper pruning and upkeep of shrubbery, trees, etc.

Interior Protection

1. Administrative, maintenance, and utility offices are considered "sensitive areas" and should remain locked and under appropriate surveillance when not in use.
2. Rooms containing audio/visual and musical equipment should be locked and under appropriate surveillance when not in use.
 - Inner doors to sanctuaries should be locked when not in use to the general public.

- Configure the audio/visual system to record activities when the sanctuary is not open to the general public.

3. Establish a written system that authorizes equipment to enter and leave the facility.
4. Bar code or tag all organizational property.

- If the nature of the object makes it difficult to tag, photograph the object and retain a copy in a “photo file.” One copy of the photo file should be on-site and a duplicate copy off-site under the business continuity plan. (Business continuity is discussed later in this document.)

Security Force

A security force for a House of Worship can be either proprietary (in-house), or contract (acquired services under legal contract).

1. Appoint personnel to lead the security detail or program that are experienced in managing security operations.
2. Conduct criminal background checks on all security personnel.
3. Uniforms consist of business like blazer, trousers, and badge or name bar identifying as security personnel.
 - Business like uniforms assist in the security function and reduce apprehension amongst congregants.
4. Communicate using 2-way radios with earpiece attachment for privacy.
5. Mini lights or Maglites are carried to provide illumination during emergencies.
6. Security Officers are trained to respond according to the security plan.
7. Training for security officers should be on-going and continuous, and include a refresher course.

Protecting Finances

Houses of Worship are large repositories of money and this risk along with growing concerns of identity theft requires immediate attention.

1. Establish “counting teams” to account for all monies after each collection.
2. Counting team members should be subjected to background and criminal history checks.
3. Transportation of money from any venue should **not** be announced, and such procedures should only be known by select members.
4. Use at least two people to transport money.

5. Any counting irregularities should be investigated by the proper authorities as soon as learned.
6. When possible, coordinate with law enforcement personnel to respond in case of any emergency.
7. Money kept on property for any amount of time should be held in a safe affording adequate protection from burglary.
8. Money leaving the premises is packaged in “discreet” bags or containers and escorted by two or more personnel.
9. Deposits in any banking facility is done on a rotating basis by days, times, and direction of travels to the banking facilities.
10. Deposit schedules are on a “need to know” basis and should only be known by select personnel.

Mailroom Protection

Mail that comes into a facility has the potential to harm people and property. These risks are reduced when proper procedures are in place to potential situations.

1. Train staff to identify suspicious mail and packages.
 - i.e. protruding wires or tinfoil, excessive tape, rigid, uneven, or lopsided envelope, fluid stains or discolorations, excessive wrappings with string, and other distractions such as incorrect titles, misspelled names and titles, or no return address.
2. Coordinate emergency response to suspicious materials with local law enforcement and fire protection services.

Daycare and Schools

Full time and even part-time educational or child care programs pose particular risks to the most innocent congregants. The following practices identify those sensitive issues and should be afforded protections accordingly.

1. Conduct criminal background checks and screening on all personnel working with minor children.
2. Establish sign-in and out procedures for all children.
3. Maintain updated roster of workers and children to include medical and/or special needs.
4. Request Identification of all adults removing children from the care of personnel.
5. Develop procedures handling court “custody orders” and temporary restraining orders.
6. Identify notification system for “lost” or “abducted” children. (Amber Alert).
7. Coordinate with local law enforcement procedures for responding to all Amber alerts.

8. Use window and door alarms to alert staff to intrusion into areas populated by children.
9. Train staff to monitor all outside and field activities.
10. Conduct periodic visual sweeps of restrooms and parking areas.

Business Continuity Planning

After a man-made or natural disaster, how fast the organization regains its business posture is of critical importance. A properly executed business continuity plan will help reduce the harm of such a disruption. For assistance in creating a Business Continuity Plan, see ASIS' Business Continuity Guideline at www.asisonline.org/guidelines/guidelines.htm.cting

1. Establish a written Business Continuity Plan (BCP) that is updated annually or when there is a change in business, environmental, or physical condition of the organization.
2. Develop plans to provide protective measures to the protection Identify vital records and resources to be protected.
3. Establish memorandum of understanding (MOU's) with other organizations to utilize resources.
4. Stock facility and off-site locations with resources necessary for business restoration.
5. Establish vendor contact lists.
6. Employ experienced Information Technology (IT) personnel for business restoration.
7. Appoint and train media spokesperson.

Special Events Planning

Special events may include conferences, seminars, or special mission event. They require attention to the protection of people, facilities, and assets. Hence, proper protection of an event requires attention to detail and the ability to call upon additional resources.

1. Conduct risk assessment of all scheduled events.
 - Identify all special holidays and events that may require additional security awareness.
2. Establish written security plan for all special events.
3. Provide proper logistics to assist the security function for the special event.
4. Security plan should address:
 - a. Attendee identification
 - b. Access control
 - c. Communications

- d. Vendor access
 - e. Asset protection of on-site products
 - f. Facility and utilities.
 - g. Parking
 - h. Evacuation
 - i. Coordination w/law enforcement, EMT, and fire fighters
- 5. Train security personnel for special event
 - 6. Provide security plan for protection of VIP's.

Overseas travel

Protection overseas can be a challenging feat, but with proper coordination and established resources, congregants can go and return to the United States with ease.

- 1. When on traveling for business, establish contact with the U.S. Consulate Office in the traveling region before leaving the United States.
- 2. Obtain Security Briefing from Overseas Citizens Services (OCS) in the State Department's Bureau of Consular Affairs.
- 3. When in country, always maintain the following information on self at all times:
 - a. Passport
 - b. Contact information for the consulate office
 - c. Contact information for your lodging
 - d. Brief list of credit card numbers and providers.
 - e. Personal medical information.
 - f. List of telephone numbers for family, doctor, etc. back home
- 4. When needing services of support such as drivers and translators, use vetted personnel identified by the Consulate office when possible.

The practices and suggestions presented herein reflect the good faith efforts and actions of security practitioners. The author(s) and/or contributor(s) do not certify or guarantee their reliability.

