



Synagogue Security: The Basics

The following "Security Thoughts" are based on a document prepared by Manfred Moses, Chair of "Watchful Westchester" of the Westchester Jewish Conference.

1. Each congregation needs to have its own custom-made security plan to address security issues. The process should include all religious and lay leaders who are involved in organizing and running the various services and activities scheduled for each facility.
2. The main purpose of all fire and security alarm systems is to accomplish the complete, orderly and safe evacuation of everyone in the building -- in the shortest, fastest and most direct way.
 - Should evacuation be necessary, get everyone at least 100 feet away from the building in order to allow for police and fire department personnel to have clear access, as needed.
 - If an alarm goes off, evacuate the building immediately and as quickly as possible. There is no such thing as a "false alarm" -- unless you happen to catch a culprit in the act!
3. The following "rules of thumb" should be observed scrupulously:

If your building alarm goes off during services -- Immediately stop whatever you are doing.

 - *Someone must take firm charge of the situation and call 911.*
 - Immediately order the evacuation of your building via the nearest exits. The rule is "Evacuate --Ask questions later."
 - Ensure arrangements exist at all gatherings in the building -- e.g., children's services, study groups, babysitting, etc.
 - Consideration must also be given to the safe evacuation of handicapped and elderly worshipers and young children.
 - Remember: confusion may occur due to worried families/friends looking for each other
4. Advance planning/preparation/training are critical in order to limit confusion. The best resources on how to evacuate effectively are your local police and fire departments.
 - Divide the sanctuary into logical sections, to match up with exit points so as not to overload a particular one.
 - Provide for "Follow Me" evacuation leaders and alternates for each section as well as signs placed at strategic locations. Arrange to have all evacuation routes kept clear of obstructions.
 - It is suggested that you prepare a simple written, non-alarming advisory on this subject, to be placed in each pew. A brief verbal announcement -- at the beginning of each service-- would also be helpful.
 - A security committee should meet regularly, perhaps twice a year, to set guidelines and evacuation routes. The committee should include the rabbi and president of the congregation, the heads of Men's Club, Sisterhood, and PTA, the chief custodian and his deputy, and the chairs of major committees such as youth activities, summer camp, school board, nursery school, building and grounds, etc.
5. Remember to do the following all year round:
 - Check/test the operation of building alarm systems and alarm bells/horns, ensuring that they can be clearly heard in all areas of your building. Also, check/test automatic interconnection with local police and fire departments.
 - Check/test all exit light units.
 - Make sure that all exits are properly identified as such.
 - Make sure that passageways to all exits are unobstructed and that there are no blockages.
 - Do not permit any gatherings or loitering in exit ways, hallways, stairwells, and on the exterior near the exits.
 - Make sure that all exit doors are unlocked, easily operable and clear.
 - Check/test all emergency lighting units.
 - Make sure that your intercom and phone systems are in proper working order.
 - Provide your custodians with large new flashlights for night-time as well as power-outage situations.
 - Provide key custodians and other staff with walkie-talkies to enhance communications between leaders.
 - Provide bullhorns for use in key exterior/interior spots.
 - Regularly inspect the interior/exterior of the buildings, shrubbery, male/female toilets, stairwells, roofs, closets, etc.
 - Arrange for a secure pre-determined location -- away from the building -- where you can meet children, relatives, friends -- should an emergency evacuation ever occur.
6. Teach your staff persons how to be aware of suspicious persons and packages -- and what to do about it.

Planning ahead is always the best policy!

SECURITY FIRST: GUIDELINES

The current international situation has engendered a renewed interest among Jewish institutions in "beefing up" their security procedures. While there is obviously no reason for us to "panic" under present circumstances, it may be prudent to acquaint ourselves with tested security guidelines -- if only for our peace of mind.

The following guidelines are designed to sensitize synagogue personnel to the considerations surrounding the handling of telephone calls, mail and visitors. While some directives assume the existence of more sophisticated security systems (e.g. buzzer system with monitor), all are valuable common-sense suggestions with relevance to most synagogues and schools.

Handling Visitors

In small congregations where only a few employees are actually on synagogue premises during the week and a buzzer system has not been instituted, visitors should be asked to identify themselves verbally through a closed door. It would then be prudent for the admitting staff member to check the visitor's identity through a window or a "peep hole." In this case, it may also be beneficial to install a silent alarm system.

As we mentioned above, security systems will vary from one congregation to another; therefore not all directives will apply to every synagogue. Nevertheless, all guidelines are helpful in delineating possible areas of concern.

Congregations may want to explore the option of having a buzzer system installed, preferably with a monitor. In most cases, this is not an expensive procedure (below \$1,000). If this is not possible, it may be necessary to keep the door locked during certain hours or to consider hiring a security guard. This is especially advisable on Sabbath and Yom Tov, where the use of a buzzer system is neither practical nor desirable.

While the following guidelines are directed primarily to those buildings with a buzzer system, they demonstrate "rules of thumb" that should be applied to all situations.

- Employees enter the office using their keys.
- Familiar visitors and employees without keys should ring at the door and identify themselves via the monitor. If identity is confirmed, the visitor may be admitted.
- If staff is not certain of the visitor's identity, the visitor should be asked for further verbal identification (name, person visiting, etc.) and then admitted once identity is confirmed.
- Unknown visitors should be asked for identification and for details about the purpose of the visit.
- The visitor may be admitted with the permission of the person being visited.
- Individuals without a reasonable purpose for the visit, or whom nobody agrees to receive, should not be allowed to enter the office.
- An unfamiliar visitor with a scheduled appointment may be admitted after identification is provided and confirmed, and upon permission of the person being visited.
- Messengers, Service and Maintenance Personnel with whom staff is acquainted may be admitted after identifying themselves on the monitor.
- Unfamiliar messengers from known service firms (those providing service to your organization on a regular basis) may be admitted after answering satisfactorily questions such as firm name, sender's name and other details, type of parcel/envelope, etc. If the answers are not satisfactory, staff should visually confirm identification through the window. The individual may then be admitted.
- Unfamiliar messengers from unfamiliar firms whose identity is verified and accepted as in the above procedure may be admitted. If the details are not accepted, these individuals should not be admitted. Instead, they should be asked to leave the item by the door. Signatures can be obtained by sliding the receipt under the door.
- Service and maintenance personnel may be admitted after prior coordination. The employee responsible for service is responsible for advising staff accordingly to avoid unpleasant incidents.
- If a service person arrives and staff have no prior advice, the individual should be asked for identification before being admitted. Such individuals should not be admitted if the reason for the visit cannot be determined.

A. Handling Telephone Threats

The use of the telephone to threaten or intimidate has become more and more prevalent. Through questioning the caller and noting down important points, problems can be prevented and the trouble maker intercepted. The following course of action may be helpful:

1. Analyze the personality of the caller making the threat.
2. Be courteous, pleasant and calm.
3. Attempt to get the caller to repeat the words and provide more detail.
4. Pay attention to the caller's voice and to background noise(s).
5. Use this list of questions to direct the conversation:
WHAT WILL HAPPEN?
WHEN AND WHERE?
HOW? IN WHAT WAY?
WHAT ARE THE REASONS? WHY ARE YOU THREATENING US?
WHAT IS THE OPERATION TRYING TO ACHIEVE?
WHAT ARE YOUR DEMANDS? WHAT CAN WE DO?
WHO IS EXECUTING THE THREAT?
WHERE ARE YOU CALLING FROM?

Record of Telephone Threat

Make a precise, written record of words used and demand(s):

Date of conversation _____ Tel. No. _____
Place _____ Precise time of call _____
Call received by _____

Note the following promptly:

Caller is ___ Man ___ Young Male ___ Woman ___ Young Female
Approximate Age _____
Voice: ___ high ___ deep ___ low ___ calm
 ___ normal ___ excited ___ strong ___ stammering
 ___ sof ___ disguised ___ influenced by drugs/alcohol
 ___ recorded

Remarks:

Language: ___ Dialect/accent _____
 ___ American English with no accent
 ___ Other language _____

Speech difficulties _____
Remarks:

Background Noises: ___ voices ___ music ___ traffic
 ___ machines ___ other _____

Remarks:

B. Handling Mail

One employee should be assigned the responsibility for handling all incoming mail, and procedures for checking the mail should be strictly observed.

All mail should be carefully examined by a responsible individual.

The following steps should be followed for mail that appears to be suspicious in the scan:

- Check manually for suspicious signs.
- Mail should not be opened until the person responsible for handling it checks with the recipient to determine if the item is expected or if the addressor is known.
- If suspicions are not resolved, check with the addressor to verify that the item was in fact sent by the addressor. If verified, the item can then be opened.
- If suspicions cannot be resolved, do not open the item. Transfer it to the police for examination.
- Items which cannot be scanned, and which are not familiar or regular, should be handled according to the steps outlined above.
- If a piece of mail appears suspicious, do not put pressure on it or bend it. This might trigger an explosion.
- Transfer all suspicious items to the police.

List of suspicious signs for mail items:

- Disproportion between weight and size of item
- Letter with no return address. (In the case of deliveries by messenger, it is advisable to confirm with the messenger who is the addressor.)
- Unknown addressor
- Something solid in the mail item which cannot be identified
- Oil signs on the envelope or package cover
- Signs of opening and repacking original envelopes or package cover
- Item smells like an almond
- There are mistakes in the address or it is written in childish or disorderly handwriting.

COMMON CHARACTERISTICS OF LETTER AND PARCEL BOMBS

- Type Mail: Foreign, Priority, Special Delivery
- Restrictive Endorsements: Confidential, Personal, To Be Opened By Addressee Only
- Visual Distractions: Fragile, Rush, Handle With Care
- Excessive Postage (Usually Postage Stamps)
- Fictitious or No Return Address
- Poorly Typed or Handwritten Addresses
- Incorrect Titles
- Titles But No Names
- Misspellings of Common Words
- Oily Stains or Discolorations
- Excessive or Uneven Weight Distribution
- Excessive Binding Material: Masking, Electric or Strapping Tape, String, Twine
- Rigid, Lopsided or Uneven Envelope
- Protruding Wires, Screws or Other Metal Parts

SECURITY CHECKLIST

All security arrangements should include the following:

- Double-check your regular security arrangements regarding the checking of non-employees coming into your building, and use caution in the acceptance of delivered parcels or letters. Critical is a re-examination of controls at your reception area.
- Do not routinely open any packages of mail that appear suspicious or unusual, and be especially cautious about mail that has no return address. Suspicious mail includes overseas mail that you do not expect, or from a sender unknown to you.
- If a person who is not known to you leaves ANY package in your office or building, treat such an object with extreme caution.
- Review your mechanical security devices, such as locks and alarms.
- All sides of your building should be well-lighted.
- Guard services, where appropriate, should be considered.
- Urge directors of your cemeteries to review, in consultation with local law-enforcement agencies, their security arrangements.

Source: http://uscj.org/Synagogue_Security_T718.html