Security for the High Holy Days and Other Special Events

The High Holy Days and other special events raise special security concerns for the Jewish community.

This chapter is designed to help Jewish community institutions prepare for holiday security in a calm and rational manner. Enhanced security does not have to come at the expense of an open and welcoming environment. And, it doesn't have to come at the expense of a balanced budget. It requires a commitment from their institution's management and constituency to make security a part of that institution's culture.

> Ideally, for security considerations to be effective, they should not begin two weeks before the High Holy Days commence.

General Recommendations

Several thoughts from earlier in this book bear repeating:

1. *Think Security*. Bear in mind that it is everyone's responsibility to keep a watchful eye on their community institutions. We must all take responsibility for security.

    a. *Leadership* should assess the risks and realities facing the institution and develop a security plan — seeking professional guidance, if needed. Of course, not all institutions run the same risk, but all run some risk.

    b. *Congregants and community members* must care about security and let others know that they do. Security procedures and your powers of observation are two of the most important assets you have.

2. Have a *security* (prevention) and an *emergency* (reaction) which includes (but is not limited to):

    a. Notifying and evacuating attendees, if necessary. Designate a meeting place to ensure that everyone is safe.

    b. Having a phone handy in case you need to call for help from outside the facility.

    See appendix on calling 911.

c. Having a person in charge of security — and vesting that person with the authority to direct a response during an incident.

3. Speak to local law enforcement about High Holy Day schedules and special events. Invite officers and the fire marshal to the facility for a security review — especially if the facilities are not the ones you usually use. Ensure that patrol officers are aware of the times during which you will be holding events when large numbers of congregants will be walking on the local streets. Consider presenting copies of schedules for distribution at your police department's roll call. A previously developed relationship with law enforcement will help facilitate this.

Contact ADL for a threat assessment.

4. Coordinate ushering and security staff. This is especially important when you are bringing in outside help for the holidays (e.g., off-duty police or a security guard). Note: ushers and security should be placed in reasonable proximity to each other so that ushers can quickly alert security to a problem.

5. A facility should have as few entry points as possible (ideally, one). However, remember to obey all fire codes and ensure adequate routes for exiting the building.

6. Ensure that existing safety devices are working and useable — especially if you are renting a facility. Video cameras should have tape, parking lot lights should work, etc.

7. Ensure that ushers understand that they play a critical role in security matters (even where there is a security staff) as they are often used to control access to the sanctuary (e.g., by taking tickets) and are in a position to spot trouble early. Meet with your ushers prior to services to make sure everyone understands his or her role and security procedures.

8. Pre-event publicity for upcoming events should be reviewed in light of security. Potential gains in audience numbers must be weighed against the security concerns created by "going public."

9. For special events where tickets are inappropriate, you may choose to use a guest list or a sign-in book. Regardless of what you choose to use, no one should enter your facility without being greeted and observed. An usher will usually function in that role.

Other sections in this manual deal with the following related and important topics:

- Suspicious people, pages 75–76
- Unwarranted interest in your facility, page 67
- Suspicious objects, page 68
- Suspicious vehicles, pages 65–67

Elements of Security for Events

Event security rests on the simple principle of *excluding* unwanted persons and *including* welcome persons. This principle is complicated by the fact that one wants to make sure that those who are to be included are efficiently processed through security and those people feel warmly welcomed and not overly inconvenienced.

At the same time, those who are to be excluded need to be stopped before entering the premises.

- Failure to exclude someone who should be excluded is considerably more dangerous than failure to include someone who should be included. The former is a life and safety issue, the latter a constituent relations issue.
- In a manner that ensures the safety of persons who are in the vicinity of the person being excluded.
- In a manner that will cause the least disturbance and distraction for security personnel.
- In a manner consistent with local, state and federal law pertaining to discrimination and public accommodations.

Steps for securing an event include

- ✓ Assessing Risk
- ✓ Establishing a Perimeter
- ✓ Maintaining a Screening Center
- ✓ Keeping Vigilance High

Assessing Risk

A number of elements go into any risk assessment; however, three stand out:

1. the existence of prior threats or incidents,
2. the extent to which the event is open to the public, and
3. the extent to which the event is publicized.

Note: There is no magic formula to determine what risk an institution has or does not have. The reality is that an event manager should try to make a series of educated guesses, in light of all the facts and circumstances known to him or her, in the hopes of thwarting an attack and mitigating damage.

Who Is Invited

Typically, an event which is open to the public will have a higher risk profile than an event which is limited to members only. Very large institutions that publicize events to their members face a similar risk to an open, public event.

It may be helpful to think about events in the following three categories:

1. *Private events* are those events to which specific people are invited from a mailing list developed by your organization personnel and who are known to your organization.
2. *Public events* are those events that any person who purchases a ticket or shows up can attend.
3. *Limited access events* are any events that are *neither* strictly public nor strictly private. Examples include: events which require tickets to be purchased by check or credit card from a central location ahead of time, or events where someone else controls the invite list.

Publicity

The next issue is whether the event should be publicized or not. An institution might face a lower risk if an event is known only to its members than if the event is publicized in a local newspaper. Larger, higher profile institutions logically face higher risks, though this is not a "hard and fast" rule as larger institutions usually possess greater resources to draw upon.

It may be helpful to think about publicity in the following ways:

- An event that is *not publicized* is one in which no public statement whatsoever (either through press release or news story) is released or published about an event.
- An event can have *controlled publicity* when the event is publicized but where *one* of the following *three* details is missing from *all* public statements and articles about the event:
  - Specific time
  - Specific date
  - Specific location

  (Some institutions, for security reasons, will require participants to call for information and require the caller to identify himself/herself. This is what we mean by *controlled publicity*.)
- An event is *publicized* if it has any publicity that exceeds these two rules, whether accidental or not.

Prior Threats and Hate Activity

Finally, it is worth discussing with your local police department and Anti-Defamation League Regional Office the nature and extent of prior threats and hate activity at Jewish institutions (locally, regionally, nationally and internationally).

In our view, the presence of prior threats or hate activity will increase the security profile of an event.

It is critical to understand that individual institutions' situations vary.

Important Note: How High a Profile Is the Event for Your Organization?

An organization running a high-profile event (Israel Day Fair), dealing with controversial issues (politics), having high-profile participants (a senator) and/or operating in a high-profile environment (e.g., during a time of raised anti-Semitism) should recognize that their risk may be higher. Institutions may wish to consider providing the highest level of security possible for any event that is publicized and/or open to the public.

A Word on Publicity

As the grid above demonstrated, publicity is an integral part of the security equation of an event. ADL makes no recommendation about whether to publicize any given event, but we urge you to understand that the more publicity an event receives, the more likely it is to attract the attention of those who may wish you or your facility harm. When you make the decision to publicize an event, it is critical that you increase the strength of your event security.

In the end, consider:

- Is the benefit of increased exposure of an event worth the cost of having a greater risk and thus needing increased security?
- Is the benefit of higher attendance worth the cost of having a greater risk and thus needing increased security?

You may answer yes to these questions, but you may also determine that the marginal cost of having half a dozen new attendees is not worth the cost of increased security.

Establishing a Perimeter

The basic element of event security involves establishing a security perimeter. Outside of the perimeter, wanted and unwanted persons mingle; inside the perimeter, only welcome persons are permitted. Your first task, then, is to identify the area you want to protect (e.g., an anteroom and ballroom, a social hall, a gymnasium, an entire building). In identifying perimeters you may wish to consider:

- The bigger the perimeter, the harder it is to secure — it takes more eyes to watch a larger perimeter than a smaller one.
- Is there a place at the perimeter to set up a screening area? If not, you may need to expand or contract your perimeter as necessary.
- Is the perimeter wide enough to prevent damage to interior spaces or persons from an attack on the outside (e.g., if an explosive device goes off outside your perimeter)? Keep in mind — you must balance the risk of attack against your ability and resources to protect and patrol the area secured.

Consider:

- If you have a high profile, controversial event, for instance, you might consider the possibility that an explosive device left outside your event could cause serious damage inside and thus you may wish a wider perimeter.
- Planners of a lower profile event in a low risk area may choose to be less concerned about that possibility.

- Perimeters do not need to make use of existing structures: you can set up an artificial perimeter to help by, e.g., using a rope line, tables or chairs organized to control traffic flow.

Once you have identified your perimeter, you should identify every way in and out of that perimeter. Include:

- Main entrance
- Emergency exits
- Kitchen doors
- Secondary doorways and entrances
- Windows
- Your security screening area

You will want to be able to secure the area so than anyone who wants to enter must go through your security screening center or is screened at a secondary screening area. Considerations include:

- Every possible way in must be *locked, guarded, and alarmed*. Remember, you must do this consistently with the fire code.
- Someone should be in charge of maintaining the perimeter and of supervising those who are assigned the task of patrolling the perimeter, guarding doors, windows, etc.
- Maintaining security when those responsible for the perimeter are distracted from their duties. For example, can your guards be distracted by:
  - A patron voicing a complaint that distracts the guard (e.g. about being denied access for want of a ticket). One solution: assign a non-guard troubleshooter, typically someone familiar with the people who are invited to an event, to assist at check-in and to whom a guard can send those with issues or complaint.

- The event they are supposed to be guarding (for example, will a notable speaker or intriguing performance have all of your guards looking stage-ward not outward?). One solution: training and supervision.
- Other responsibilities, such as being required to leave a post to assist in a medical emergency (for example, if someone falls ill, will your entire guard staff be off of their posts?). One solution: have a medical emergency plan in place.

Once your perimeter is established, it is wise to clear the area inside of the perimeter and inspect the entire space, looking for anything — a device, a person — that may have been hidden before you established your perimeter. This would be, for example, when you let an explosives-detection dog sweep the area. Make notes of what is there that might later cause suspicion. Once the perimeter is swept, *only* those cleared through your screening center should be permitted inside.

Maintaining a Screening Center

Your screening location should be designated as a location when people are cleared to enter your perimeter. It may be the place where a ticket is checked, a guest list consulted, where metal detectors are deployed — whatever you determine is necessary for your event. Your local police department can be of assistance in making this decision. At the very least, everyone should be visually inspected for suspicious characteristics and behaviors.

A few considerations:

- Entrance credentials — any ID that permits one to enter an event (e.g., table cards, event ID cards, etc.) — that are handed out at the check-in center should be distributed by staff, not left alone on a table for collection. We caution against having unstaffed name tag tables.
- It is important to secure or guard entrance credentials from theft. We also suggest that where name tags are displayed on a table, for ease of the staff checking people in, someone be assigned the job of ensuring that no one steals entrance credentials.

- For entrance credentials that are used to facilitate reentry to an event, consider collecting those credentials from people who will not be returning to the event. Your security will be compromised if someone can use a badge that he/she retrieved from a trashcan outside of the event. This is especially true of special credentials, such as press credentials.

Your security staff should:

- Ensure the perimeter remains intact
- Query anyone who is without a displayed entrance credential
- Look for unattended bags and packages
- Watch or report suspicious behavior
- Understand their role in an emergency, including when to leave their post and when not
- Understand that they are guarding an event, not participating in it or watching it. Therefore, they should be watching the crowd and the perimeter and not focus on the performer, speech or event.

Security concerns for special events, parties, *simchas* may include the following.

- Assign ushers who can maintain a watchful eye and who understand that their job includes security.
- Not publish the name of a child or couple in any public newspaper or on the sign in the entranceway or on the street.
- Do a security sweep — a walk-through — before the event, no matter how low profile.
- Gifts set down become unattended packages: they should be kept on a special table and supervised.

This guide is intended to help institutions become aware of basic security considerations. It is not intended to provide comprehensive, institution-specific advice on security matters nor is it meant to replace the advice of a security professional. For comprehensive, institution-specific security advice, a security professional should be consulted. ADL specifically disclaims any and all responsibility for, and is not responsible for, any loss or damage arising out of the use, nonuse or misuse of this information

Web site: **www.adl.org**