From the Editor

It is a sad sign of our times that a publication of this kind must become part of the library of reports, studies, guides, thoughts pieces, guidelines, and manuals for JCCs, Ys and camps produced by JCC Association of North America. Yet here we are.

Security is now embedded into the everyday operations of JCCs. It’s part of the checklist of program development (“what are the legal, insurance, and security implications of having this event or running this program?”) Without both the reality and perception of a safe and secure environment, the JCC business model does not work.

Even without the 2017 security crisis, the rise of hate in the world, so much of it disproportionately directed at Jews and our institutions, would have likely required us to develop this publication. In many communities, JCCs are the most visible evidence of our presence, of our success. For 99% of the public, our presence is welcome and cherished, in the same way JCCs welcome and cherish that public. But against the one percent who hate, and the even smaller number who would act on that hate, we must protect ourselves.

While not being the final, last word on everything concerning security at JCCs, Ys and camps, this publication is extensive. It is dense. There are checklists in some sections, but it is primarily a deep thought piece that will raise questions for your deliberations. It is made to make you think. Do not try to read it quickly. Use it as a source of discussion for the security committee (Section I) it suggests you establish staffed by a lead security professional (Section K) at your agency or for your community.

It addresses some overall security concerns uncovered by the wide-ranging 2016 JCC Security Survey. Information is to be found on more rarely covered aspects of security like guard force management (Section G), off-site meetings and events (Section J), and rapid security escalation (Section F).

We are indebted to the author, Paul DeMatteis, for his work these past two years. He visited many JCCs and camps to learn who we are and how we operate. We could have had no better partner, and I personally want to thank him for what I’ve learned from him.

Thank you to those JCCs and camps who welcomed Paul in 2017, to the JCC Maccabi team and the leadership of the 2017 JCC Maccabi host communities of Albany and Schenectady for his immersive education there, to the development, and marketing and communications departments of JCC Association of North America for all their expertise, and to Dr. David Ackerman for his editing work on the camp bulletins. Special thanks to the Goldhirsh-Yellin Foundation of Los Angeles, CA for its financial support, without which this would not have been possible.

Use this publication well, use it wisely, and let us hope for a time when we never have to use it again.

David E. Posner
Vice-President, JCC Association of North America
Disclaimer

THIS PUBLICATION IS INTENDED TO PROVIDE INFORMATION AND GUIDANCE TO JEWISH COMMUNITY CENTERS (“JCCS”), YM & YWHAS, AND CAMPS ABOUT HOW TO APPROACH PLANNING FOR SECURITY READINESS. IT IS INTENDED FOR USE BY JCCS, YM & YWHAS, AND CAMPS ONLY.

THIS PUBLICATION DOES NOT PROVIDE COMPREHENSIVE, INSTITUTION-SPECIFIC ADVICE ON ANY ASPECT OF SECURITY READINESS NOR DOES IT PROVIDE ANSWERS TO EVERY QUESTION ABOUT SECURITY READINESS. JCCS, YM & YWHAS, AND CAMPS ENGAGING IN SECURITY PLANNING SHOULD ENGAGE PROFESSIONALS TO HELP DEVELOP AND IMPLEMENT AN INSTITUTION-SPECIFIC SECURITY PLAN. THIS DOCUMENT IS NOT INTENDED TO SERVE SUCH A PURPOSE.

SOME OF THE TOPICS DISCUSSED IN THIS PUBLICATION MAY BE SUBJECT TO FEDERAL, STATE/PROVINCIAL, AND/OR LOCAL LAWS, CODES AND REGULATIONS, WHICH CAN FREQUENTLY CHANGE, AND THIS PUBLICATION IS NOT INTENDED TO AND MAY NOT PROVIDE CURRENT, UP-TO-DATE INFORMATION REGARDING LEGAL AND/OR REGULATORY REQUIREMENTS. JCCS, YM & YWHAS, AND CAMPS SHOULD CONSULT WITH THEIR OWN LEGAL COUNSEL WITH REGARD TO LEGAL AND REGULATORY COMPLIANCE ISSUES.

THIS PUBLICATION IS NOT IN THE PUBLIC DOMAIN. JCCS, YM & YWHAS, AND CAMPS MAY USE, REPRODUCE, OR DISTRIBUTE THIS PUBLICATION ONLY WITHIN THEIR OWN ORGANIZATION. WITHOUT THE EXPRESS APPROVAL OF JCC ASSOCIATION, NO INSTITUTION SHALL PUT, DISPLAY, LINK OR MAKE AVAILABLE THIS PUBLICATION OR ANY OF ITS CONTENTS ON THE INTERNET OR INTERNET PLATFORMS. INSTITUTIONS SHALL NOT MODIFY, PUBLISH, TRANSmit, TRANSFER, SELL, CREATE DERIVATIVE WORKS FROM, DISPLAY OR IN ANY WAY EXPLOIT ANY OF THE MATERIAL, IN WHOLE OR IN PART, EXCEPT AS OTHERWISE EXPRESSLY PERMITTED BY JCC ASSOCIATION.

THIS MATERIAL IS PROVIDED FOR EDUCATIONAL AND INFORMATIONAL PURPOSES ONLY, AND JCC ASSOCIATION AND THE AUTHOR OF THIS PUBLICATION MAKE NO REPRESENTATIONS, GUARANTEES, OR WARRANTIES OF ANY KIND, WRITTEN OR ORAL, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, WARRANTY OF NON-INFRINGEMENT, OR ANY OTHER STATUTORY WARRANTY. JCC ASSOCIATION AND THE AUTHOR HAVE NO OBLIGATION TO SUPERVISE, MONITOR, REVIEW OR OTHERWISE ASSUME RESPONSIBILITY FOR THE USE OF THE MATERIAL IN THIS PUBLICATION, AND THEY ARE NOT RESPONSIBLE FOR OR ARE LIABLE ANY INJURY, LOSS OR DAMAGES TO PERSONS OR PROPERTY ARISING FROM, IN CONNECTION WITH OR RESULTING FROM THE USE OR MISUSE OF THIS MATERIAL.

© JCC Association of North America, 2018
SECTION H. SITE INSPECTIONS
INTEGRATING SITE INSPECTIONS INTO A SECURITY PROGRAM
WHY REGULAR INSPECTIONS ARE IMPORTANT
Who Should Conduct Inspections................................................................. 56
Security Inspection Protocols.................................................................... 56
What to Look for During an Inspection....................................................... 56
Developing a Unique Security Checklist.................................................. 57
Visual Inspection of Exterior Areas and Conditions.................................... 57
Visual Inspection of Interior Areas and Conditions...................................... 57
Inspection of Security Systems and Conditions
(Security Systems Inspections May Require More Than One Individual)... 58
Questions and Calls to Action.................................................................... 58

SECTION I. GUIDELINES FOR DEVELOPING A SECURITY COMMITTEE
Projects........................................................................................................ 60
First Steps .................................................................................................... 60
Pitfalls to Avoid............................................................................................ 61
Questions and Calls to Action.................................................................... 61

SECTION J. SECURITY GUIDELINES FOR OFF-SITE MEETINGS AND EVENTS
General Concept.......................................................................................... 64
Planning a Smaller Off-Site Meeting........................................................... 65
Larger Event Security Strategy................................................................. 65
Large Event Security Checklist.................................................................... 67-72
Event Opening Questionnaire (Two Weeks From Event)............................. 73-74
Conclusion.................................................................................................. 75

SECTION K. SECURITY JOB DESCRIPTION
CREATING A JOB DESCRIPTION FOR THE LEAD PROFESSIONAL
OR CONSULTANT OVERSEEING SECURITY AT A JCC FACILITY
Job Description ............................................................................................ 78
Background .................................................................................................. 78
Qualifications ............................................................................................... 78
Experience .................................................................................................... 78
Education ...................................................................................................... 78
Certifications ................................................................................................. 78
Basic Interview Questions............................................................................ 78
Lessons Learned........................................................................................... 79
Hiring a Security Consultant........................................................................ 79
Questions and Calls to Action.................................................................... 79

SECTION L. VISITOR MANAGEMENT/UNAUTHORIZED PERSON ON PREMISES
Guidelines for Visitor Management.............................................................. 82
Conclusion for Visitor Management............................................................. 83
Guidelines for Unauthorized Person on Premises......................................... 83
Conclusion................................................................................................... 83
SECTION M. SUSPICIOUS MAIL IDENTIFICATION AND RESPONSE
Identifying Suspicious Mail or Packages ................................................................. 86
Response to Suspicious Mail or Packages ............................................................. 86

SECTION N: ADDITIONAL RESOURCES
Links to Additional Resources ............................................................................. 88

PREVIOUS RELEASED SECURITY BULLETINS
SECURITY BULLETIN 1, MAY 2017
Executive Summary: Foundation for Establishing a Security Mindset ...................... 90

SECURITY BULLETIN 2, JUNE 2017
Target-Hardening and Early Detection (Training Curriculum Included) .................... 96

SECURITY BULLETIN 3, JUNE 2017
Security for Summer 2017 .................................................................................. 103

SECURITY BULLETIN 4, JUNE 2017
Emergency Response Plans and Providing Safe Havens .......................................... 107

SECURITY BULLETIN 5, AUGUST 2017
Protest Rally Preparedness for JCCs .................................................................... 112
SECTION A

INTRODUCTION TO SECURITY MANAGEMENT:
BALANCING SECURITY AND OPERATIONAL NEEDS
SECTION A. INTRODUCTION TO SECURITY MANAGEMENT
BALANCING SECURITY AND OPERATIONAL NEEDS

An effective security management program relies on good business practices. It also requires the guidance and support of senior management. It must have a logical reporting structure, accountability and written goals and objectives that consider organizational culture and customer service. A good security management program provides comfort and safety for staff and participants.

In most organizations, security directors and security managers report to an executive with little or no formal experience in security or emergency management. This executive rarely has the time to dedicate to security issues. In some cases, these directors and managers are in their first private-sector security positions. This staffing structure is unique to the security field, and it is prevalent among both large and small organizations and corporations. This staffing structure creates a knowledge gap and puts organizations at a disadvantage in implementing and managing a balanced security program. This manual will help bridge that knowledge gap and offer guidance in the creation, implementation and management of a balanced security program.

Under these circumstances, it is beneficial to have a well-planned and documented security management program. This manual was developed for JCC executives who wish to gain insight into security management, as a roadmap for novice security professionals and as a tool to be used by experienced security professionals to develop, document, implement and maintain an effective program.

This manual is also intended to relate stories, promote conversation, create unity and educate individuals on the value of a strong security culture. In today’s dynamic world, security is everyone’s responsibility. This manual presents security-related material in terms that can be appreciated by a wide spectrum of participants.

The material in each section is organized in order to explain various types of security exposures and offer multifaceted recommendations for mitigating those exposures to within acceptable levels. Examples of, and reasons for, security successes and failures accompany training materials that will assist you in preparing for emergencies and crises, as well as make your environment security-conscious.

Primary Goals and Objectives: Introducing a Four-Point Strategy

There is no single thing that ensures the safety and security of any facility or campus. Rather, it is the cumulative impact of proper planning and implementation in four primary areas that yields the best outcome:

• **Look like and be a hard target.**
  People looking to do harm will choose the easiest target. If it looks hard to gain access to your JCC, a potential perpetrator will turn away and look for something easier.

• **Use early-detection systems (cameras, alarms, alerts to staff and members, threat monitoring, etc.).**
  The sooner you can identify a “bad actor,” the more time you have to respond; each extra minute provides an extra margin of safety. Identifying a threat at the entrance to the parking lot rather than at the entrance to the building can mean lives saved.

• **Implement appropriate response plans and systems.**
  Having plans for the types of threats you anticipate is the first step. Systems to notify staff and membership and the ability to quickly lock down your facility are other key components. Ongoing staff training, drills and simulations are also integral to the success of any plan.

• **Provide safe havens or an escape strategy.**
  Deterring a threat from entering your JCC is a goal, but it is essential to have a strategy in place to exit the facility and to provide multiple forced-entry-resistant locations within the facility in which to shelter in place while waiting for law enforcement to arrive.

A basic risk assessment helps protect against a random attack because it provides a snapshot of current and past threats and offers recommendations for mitigating those threats. A bad actor might decide to go on to another target when he perceives that the defenses described in this document are in place.
Protecting against a dedicated adversary will require additional resources. A bad actor seeking to harm a particular person or facility will not turn away to an easier target, but rather will be focused with determination on the intended target. Because of the dedicated nature of this type of attack, you must assume that the actor will go to greater lengths to defeat defenses, and that he will be willing to alter plans to take advantage of opportunities as they arise.

Organizations must pay constant attention to threat monitoring and analysis, identifying suspicious activity, hostile surveillance and global events. An appropriately designed and managed security management program should emphasize threat monitoring and analysis. When a particular reason for concern presents itself, there should be mechanisms in place to rapidly raise the level of protective controls and response capabilities as warranted by the current threats and conditions.

**Minimum Security Controls and Risk Management Strategy**

If your facilities were not closely associated with Jewish and Israeli culture and values, how much security would be required? What controls would be required for a nonsectarian facility?

Such a facility would traditionally require a basic level of security to promote a safe environment for participants, to protect assets and to limit access to the facility and particular services. It would require access control for staff, members and visitors; monitoring of rear entrances and exits, emergency egress doors and designated sensitive areas; the ability to respond to emergencies; controls for keeping vehicles away from playground areas and additional measures to protect children. It would also require the appointment of someone responsible for all aspects of security and emergency management. This basic level should be your starting point.

In today’s world, JCCs and other Jewish institutions must give additional consideration to the sectarian nature of their facilities and the fact that they offer diverse services, often on a large scale. The services and the risk factors associated with your organization must be evaluated and calculated to develop a sliding scale of security controls.

This manual includes guidelines for developing, implementing and maintaining basic minimum security and risk management controls. It also includes escalation strategies in Section F for expanding permanent or placing temporary security enhancements at your facility when they are required to meet immediate threats.

---

**Lessons Learned: Security Failures and Recommendations**

This section provides examples of security failures and recommendations for avoiding known pitfalls. These examples can also serve as talking points for emphasizing effective security controls during training sessions.

**LESSON 1:**

Organizations will boast about their security programs, or they will claim they have never experienced a security problem or loss.

For example, a global company was asked how many laptops were lost annually. Their response was “none.” This seemed unlikely. It turned out that the company did not have a requirement to report, or a mechanism for formally reporting, missing laptops. Investigation revealed that the number of laptops that went missing annually was actually quite high.

Sometimes, a security program appears on the surface to be functioning well because there is no monitoring of whether or not it is functioning at all. Often, it is just a matter of luck that nothing has happened or that an institution is unaware of what has happened. This is true in all aspects of security management: event security, building access control, computer security, fraud, etc.

**LESSON 2:**

People are often asked during investigations of high-value theft, employee wrongdoing, hostile work environment, fraud, etc.: “Did you think this could happen?” The majority respond affirmatively.

When asked, “Why did you fail to report your concern prior to the event?” the following responses are common: “I did not think it was my responsibility,” “I did not know who to speak with,” and “I did not want to get involved.”

Safety and security should be everyone’s responsibility, and general and particular responsibilities should be clearly defined within employees’ scope of work.

All employees must know their responsibilities and how to report critical information. Security exposures should never be ignored. Small security exposures—exiting through a rear door, wedging open a door that is usually locked, failing to check IDs, allowing exceptions for privileged individuals, etc., have sometimes led to large, and sometimes tragic, security problems.

Section B of this manual addresses security awareness and establishing a security-aware culture.
Lessons Learned, continued

LESSON 3:
A global public company was targeted by Al Qaeda (a dedicated adversary) several years after 9/11. Al Qaeda’s advance team conducted weeks of mobile surveillance and surveillance from public space areas, acquired official literature from building lobbies, questioned employees outside the building, gathered information via the internet and collected published pictures and information.

Al Qaeda used this surveillance to create a detailed assessment and multiple attack plans against the organization’s headquarters building. The majority of Al Qaeda’s plans focused on exploiting smaller security exposures. Most of the exposures were the result of privileged behavior, efforts to avoid inconveniencing employees, marketing and perception issues, disregard of reasonable security exposures and the perception that existing security was adequate.

Bad actors conduct surveillance, pay close attention to your security controls and procedures and look for the simplest solutions to do the most damage.

Note that identifying hostile surveillance is one of the most effective ways an organization can protect itself against a bad actor (Section B). This Al Qaeda surveillance was conducted prior to 9/11; hopefully today a hostile surveillance event would be quickly identified.

Top 10 Reasons Why Security Fails
A study conducted at John Jay College of Criminal Justice showed that the issues below account for the top 10 reasons security fails:

- Misconceptions about threats and vulnerabilities
- Lack of standards, guidelines and policies
- Lack of security awareness programs
- Vague or undefined responsibilities
- Lack of auditing and monitoring
- Failure to test security systems and controls
- Limited or no enforcement and/or disciplinary actions
- Exceptions, privileges and personal agendas; too many layers of influence
- Poor communication between staff/management and among departments/divisions
- Lack of management involvement and support

Questions and Calls to Action
1. How has your JCC incorporated the four-point strategy into its security posture?
2. What is the JCC’s plan for security escalation in the event of a heightened threat situation? (Refer to Section F for guidance before answering question.)
3. Does the JCC meet minimum security controls as outlined in this section?
4. To what extent does JCC staff report exceptions to the normal operating environment? What might be the reasons they do not?
5. Considering the top 10 reasons security fails, how would your JCC rate? Be honest in your assessment.
SECTION B

SECURITY AWARENESS

ENHANCING AN EXISTING SECURITY PROGRAM BY PROMOTING SECURITY AWARENESS

ESTABLISHING A SECURITY-AWARE CULTURE AND REPORTING STRUCTURE
An organizational culture that promotes security awareness—a culture in which staff and participants identify and report suspicious persons, activities and conditions—will greatly improve a security program.

When management is vocal about the importance of security and the safety of the organizational environment, staff and members will participate more fully in a security program. Effective security does not happen in a vacuum. It cannot be one person’s responsibility; it is everyone’s responsibility. Everyone at a facility can positively or negatively impact its security program. When everyone participates, the general level of security dramatically increases. Management must set the pace and set a good example. When management takes exception to security practices, it diminishes staff and member participation, which could result in members routinely bypassing security controls.

During the investigation of a security event, it is often the case that a number of people had pre-existing knowledge of the circumstances that led to the event. Examples of these types of events include fraud, theft, misuse of services, potential for an active shooter, workplace violence, terrorism, etc. In such cases, something that could have been avoided happened because of poor communications and/or protocols.

**To be successful, this strategy requires six key components:**

- Management should promote the following of existing security rules and regulations.
- Management should assure staff that their observations are welcome.
- Management should instruct staff on what to do and where to report suspicious or dangerous conditions.
- Staff should be instructed to be aware of their surroundings.
- Staff should recognize suspicious indicators and follow their instincts.
- Staff should be certain that information and actions taken will be confidential and that actions taken will be fair and balanced.

**Staff Training**

Permanent, seasonal and consulting staff—long-term and new, full-time and part-time—should participate in an initial orientation program that highlights the benefits of an active security awareness program and makes clear each of their responsibilities. If presented appropriately, staff and members should feel integral to the program, proud of their combined efforts and empowered to provide a safer environment for all participants. This training will assist participants in recognizing suspicious and dangerous situations in their personal and professional lives. Learning to take prompt action when they see something will keep them, their friends and their families safer outside of your JCC.

Often, unacceptable security conditions are created by individuals who are unaware of the negative impact they are having on overall facility security. Someone propping open a backdoor used for fire egress to improve ventilation, sharing an ID card or opening a back gate to provide faster access to a vehicle might never think of the serious security impact of those acts. Also, someone witnessing a suspicious or negligent act who does not feel compelled to report it might not think about how it could affect the community.

When hiring new staff members or consultants, security awareness training should be part of the onboarding process. Present security awareness training regularly and/or when new security threats or conditions present themselves. At a minimum, conduct two training sessions or presentations annually.

To ensure that your security awareness presentations are informative and empowering, it is critical to present the information appropriately. Some consultants and law enforcement departments can present facts in a very harsh manner. The truth must be told, and difficult questions will arise. Each potential threat should be presented in a factual and realistic manner. Emphasize each threat’s likelihood in a professional matter and offer recommendations for best actions. Avoid presenting the information dramatically or loudly in order to gain attention. Some things to avoid:
• If using PowerPoint or paper, avoid using screenshots or black paper with white lettering. If the presentation is visually overwhelming, it can be distracting and individuals will not fully benefit from the information.
• Do not use graphic photographs from past events.
• Refrain from focusing on what will happen to participants if quick action is not taken.
• Avoid conducting intense live exercises with law enforcement and staff. For some individuals, seeing guards dressed in tactical gear with weapons could be as intense as a real event.

Lessons Learned: Security Awareness Examples
Following your instincts is a key component of security awareness. Without immediate reporting and analysis of all security-related information, it is difficult to detect patterns, foresee potential events and take protective actions.

LESSON 1
Senior management at a global organization was under the assumption they had very few security-related problems at their 200 U.S. field offices. During one of their annual meetings, a group of approximately 1,000 participants answered several questions. The responses established that most, if not all, locations had security-related problems and threats that staff had not reported to the U.S. headquarters. Reasons given included that staff members did not know they should report the incidents in question and that they did not want the main office to think they could not handle their own security-related issues.

LESSON 2
In a similar situation, a U.S. global bank’s regional executive refrained from transmitting what was perceived to be negative information to corporate headquarters. The executive gave similar reasons for this failure to report; it was also made known that if senior management knew of the problems, they might reduce funding or opportunities in that region.

LESSON 3
Similar situations and responses have been noted following active shooter events. Persons with knowledge of a pending event failed to report it for fear of getting into trouble or causing serious problems for others. A successful program must make all participants aware that this type of information is critical and must be presented to management. Management must assure staff that reporting security-related information is the right thing to do, that all information will be confidential, that actions taken will be balanced and that all parties will be treated fairly.

LESSON 4
A businessman who traveled extensively worldwide had a difficult and lengthy trip planned. One leg of the trip caused him particular concern. He asked questions and sensed some confusion and disconnect, but eventually just confirmed plans for that leg of the trip. He left home worrying that he was ignoring his instincts. The end result was that the executive wound up stranded in a one-gate airport in the middle of Africa at 1 a.m. without a ride to his hotel, which was 100 miles through the jungle. In this situation, the executive did survive being stranded, and eventually made his way (in a very unsafe manner) to his final destination. When reflecting upon what could have happened that day, he vowed not to ignore his instincts in the future.

Foundation for Establishing a Security Mindset
Security awareness training programs for your location should reflect your individual needs. There are many potential topics and many different ways to present material. Regardless of whom develops and presents the program, senior management should review it to ensure that the subject matter, material and delivery process is appropriate for your organization. Even if law enforcement, DHS, a security consultant or a volunteer familiar with security management develops and presents the material, senior management should conduct a review. Ideally you should be able to evaluate the entire presentation prior to presenting it to your staff, membership or participants.

Your presentation should empower participants and create a team approach to providing a safer environment. Participants should leave knowing that they are not helpless and that they can make a difference. All participant questions should receive answers during your presentation. If an answer is not readily available, tell participants that their questions will be answered within 24 hours. If no questions are raised, the presenter should be prepared to introduce questions that will spark conversation. The resulting conversation will reveal the level of participants’ understanding.

Participants will be more eager to participate if they truly understand the threats they face and the benefits of the program. Questions that might be anticipated when sessions are announced include: “What are we looking for?” “Why is such diligence required?” and “How will this improve our safety?”
Understanding the Hostile Act and Actor

Building your strategy around the following aspects of the hostile act and hostile actor is vital when creating a successful program.

A hostile act is an attempt to use deadly force on one or more individuals. It can result from an incident involving a random active shooter; a terrorist; participants in a domestic, workplace or criminal dispute; or any other act during which there is an attempt to use deadly force. Such acts can be, and typically are, completed within four to seven minutes. You must have prepared in advance to manage such an incident if there is hope of mitigating damage and loss.

Time is the enemy of hostile actors. The actors know that once their presence is known (breaching a fence or entry, an explosion or a shot fired), they have limited time to complete their mission. The more warning you have, the better you will be able to limit the impact of an event. Speedily identifying a bad actor dramatically decreases his ability to harm a larger number of individuals.

Adversaries use hostile surveillance as a tool to ensure success. It is thought to have been conducted before all known attacks. It is also an opportunity for us to become aware of bad actors’ interest and report it to law enforcement. Identifying and quickly reporting hostile surveillance to law enforcement is the best way prevent an incident. In a public area this might be difficult, but on private property there are many opportunities to identify individuals who do not belong and who are focused on observing members and/or security procedures. Someone watching how we respond to unauthorized access, a bomb threat, a fire drill or a suspicious package can provide a great deal of valuable information to bad actors.

Security Awareness and Training Curriculum

Knowing what constitutes suspicious activity is a first step. Some typical indicators are listed below. Please know that this list is not exhaustive; if you have had incidents at your JCC or have been notified by law enforcement of particular local issues, add other relevant indicators to this list.

Watchers

- Someone watching members or staff arriving and/or departing, opening and closing procedures, access control procedures, back doors that are kept open, children at play, etc.
- Someone watching and/or taking pictures of the buildings, entrances, parking areas, security controls, children, evacuation drills, etc.
- Someone watching the facility from neighboring buildings, adjacent areas or roads, etc.
- A drone flying over or near your JCC
- If water-accessible, someone monitoring your property or security protocols from a boat
- Someone who does not appear to fit in asking for directions at the gate or near property lines

Strangers and Strange Behavior

- Someone you don’t know carrying bulky and/or heavy bags
- Someone you don’t know looking angry and/or annoyed
- While off-site, anyone showing unusual interest in your presence and/or inquiring about the JCC or its security controls
- A vehicle, driver or idling engine directly across from a sensitive area of the facility for no apparent reason
- An individual walking through your property who appears to be observing your security equipment, operational procedures, staff or membership movement, etc.
- Someone on your property asking for directions for a delivery or doing a repair
- An individual carrying equipment inconsistent with routine JCC activities (e.g., military-type equipment, a GoPro, etc.)

Anomalies

- Any indicators that unauthorized persons might have been on your property
- An unlocked door that opens to a room in which hazardous chemicals (chlorine, gasoline, propane, etc.) are stored
- Finding trail cameras on your property
- Suspicious calls, inquiries about security and emergency management or requests for opinions on sensitive matters
- Something new in an area or a building that could indicate the presence of an unauthorized person on your property
- Something missing that might indicate an unauthorized person on your property
- An unattended area that is usually staffed by reception or security
- Something moved to enable an individual to reach an upper window or access point
Security Violations

- Someone walking past reception or security without being properly identified
- An unauthorized individual in a restricted area (childcare, offices, swimming pool, etc.)
- A person accessing the facility via a fire exit door that should have been locked
- A rear door that has been propped open
- Someone attempting to break or in the act of breaking any established security protocols

Membership Training

During membership presentations, introduce prospective members to the idea that security awareness is an integral part of the JCC world and let them know that they will be asked to participate in four basic ways:

- Follow all the rules and regulations of the club to help maintain a safe environment.
- Be alert to their surroundings.
- Report anything suspicious to a designated person.
- Participate, if possible, in in-house security awareness briefings conducted by law enforcement and security experts.

In general, most people will comply with security regulations if they understand their responsibility and the importance of the regulation. Comprehending the reason for the regulation—to keep them safer—provides personal value to the individual. You will never get 100 percent participation. Without a proactive program, most organizations probably have a 1 to 3 percent participation level. If a security awareness program raises this level above 70 percent, your overall security will be greatly enhanced.

Conduct staff and membership training separately. Staff members who wish to participate in member training should be allowed to do so. However, because of the detailed information relating to staff responsibilities and planned responses discussed at staff training, members should not be allowed to attend staff training.

To provide a generic training session to membership, use local or state law enforcement and/or DHS resources. JCC management should provide input to ensure that pertinent site information is appropriately presented.

Conclusion

Developing a security awareness culture is the most economical way of quickly and efficiently enhancing your overall security. Being alert and reporting suspicious activity, along with prompt analysis and response, can help avoid serious security issues. In today’s world, security is everyone’s responsibility.

Two things in particular to be mindful of are to:

- Know what to look for and where to report it
- Avoid ignoring your instincts

Questions and Calls to Action

1. What do you do to include security awareness as part of staff training and membership presentations?
2. What procedures are in place to assure the greatest likelihood of staff members and participants reporting anomalous behavior?
3. Do senior leaders model the kind of respect for security you need to be effective?
4. Do you know the primary go-to people from the local branches of the FBI, the DHS, law enforcement and other uniformed services so that they are readily available to assist in a security event and to make presentations as needed and appropriate to staff, members and participants?
5. What is included in new staff onboarding about security?
SECTION C

RISK MANAGEMENT

RISK MANAGEMENT IS A BUSINESS PROCESS
SECTION C.
RISK MANAGEMENT
RISK MANAGEMENT IS A BUSINESS PROCESS

From the simple to the complex, we conduct personal risk assessments every day. “Should I take an umbrella?” “Is it safe to travel to that area?” “Should I let my children attend that concert?” Managing a JCC is a complex process, and business risk management, as it relates to the safety and security of your operation, is already part of your daily life. Although this guideline focuses on security risk management, a similar process applies to evaluating financial risk, medical risk, construction risk, etc.

Providing for all of the possible security problems that could arise can be a daunting task. This section is meant to help you organize and structure your risk management process. It takes a common-sense approach to risk management by outlining tools and concepts that you can use to detect and mitigate unacceptable levels of risk.

Tools and Concepts
Below are some processes that should be part of your risk analysis:

• An examination of event history, including incidents related to operational procedures, adherence to procedures, electronic systems, physical controls and employee compliance to identify root causes
• An assessment of likelihood, determination of consequences and impact (criticality) and analysis of findings
• A decision regarding the organization’s comfort level for risk and performance of a gap analysis
• Mitigation of unacceptable exposures and continual monitoring of the potential risks and/or hazards

Risk cannot be managed unless it is first correctly identified. Risk management is a dynamic (and endless) process. While independent risks and hazards may have a life cycle, the process of identifying and analyzing findings is continuous. Risk management is not a matter of making a checklist; rather, it is an analytic business process that requires continuous attention and maintenance. It relies heavily upon a business and management culture of identifying and reporting risks and hazards in a timely fashion and addressing those risks with structured decision-making. Under traditional risk management protocols, ownership of identified risk is assigned to various individuals and groups, who become responsible for the risk management process. In a JCC environment, risk ownership should be assigned to the executive director and/or his or her designee.

Note that determining the likelihood of a security event (terrorism, anti-Semitic activity, etc.) for any JCC location is problematic because of domestic and international threats to the entire Jewish community. In addition, certain criminal risks, such as workplace violence, custody issues, sexual crimes and crimes motivated by mental health issues, cannot be predicted. To assist in attempting to quantify the likelihood of such events, analyze local event history and threats. Threats particular to your JCC should be given weight in this process (such as a nearby chemical facility or other high-risk business, freight train tracks or a local potential for wildfires).

Some areas may be at a higher risk than others for some types of security-related problems, but recent security events have demonstrated that location is not a key indicator in tragic events. Criticality can be more effectively determined and measured. A theft in a JCC’s locker room is unfortunate, but not as critical as other types of security events.

Once a risk management program has been established, make ongoing efforts to:

• Enhance risk monitoring and reporting structures
• Establish better risk identification processes and procedures
• Improve communications concerning risk
• Provide more timely responses to critical issues
• Promote more risk-based decision making

Measuring and Assessing the Various Types of Risk

How do you identify your potential risks? Dividing risk into six categories—acceptable, unacceptable, insurable, undetected, ignored and security negligence—is helpful in defining your risk criteria, and doing so will assist you in deciding how to address risk. These are not definitions; rather, these terms will provide guidelines to assist you in conducting risk assessment surveys and developing a security risk management program.

• Acceptable risk encompasses the risk of loss your organization can tolerate. There is a risk, but the likelihood and impact of an event occurring is very low. It must be continuously monitored to ensure it does not become unacceptable.
• **Unacceptable risk** is beyond your culture’s tolerance for loss. The security problem is foreseeable, and the impact will affect your JCC adversely. In such instances, controls or systems must be developed and implemented to eliminate or lessen risk so that it falls within an acceptable level. Unacceptable risk can include parking lot crime, hate-related graffiti, a rear exit door near the gymnasium being propped open to provide access to an unauthorized person, etc. The above conditions would require a timely, reasonable and effective security response.

• **Insurable risk** is also beyond your organization’s tolerance. Some types of risk can be mitigated by developing a relationship with a secondary party (insurer) to limit your risk for a fee. Depending on the issue, this may not totally insulate you from adverse press and/or damage to your organization’s reputation. Even though an insurer is involved, the risk must be continuously monitored and evaluated and additional actions must be taken if required. The insurer may have requirements of its own to mitigate risk.

• **Undetected risk** could not be detected and/or was not detected. The risk levels exist but have not been identified correctly. Once the event occurs, issues must be addressed without appropriate preparation. This is most prevalent when the appropriate level of attention is not allocated to security and risk identification and management. This can include an alarm system that is no longer functioning, a video recording system that is not recording, unauthorized persons accessing your facility, dangerous road conditions near playgrounds, back facility doors propped open, security guards working without appropriate direction, etc. Ongoing efforts must be maintained to ensure that this category of risk is kept to a minimum.

• **Ignored risk factors** can be extremely problematic and have a considerable impact on your organization. In this category, risk factors are known but ignored. This can occur when risk identification programs and risk assessments are merely ceremonial. It can also occur when people who are unaware of the potential for loss, or are simply unconcerned with security issues, are responsible for security oversight and/or conduct risk assessments. Ignored security issues are the most dangerous category. They can occur when a trusted employee makes a poor or uninformed decision that could result in a major security problem. The best control to limit exposures to ignored risk factors is an active risk identification and security management program supported and driven by senior management.

• **Security negligence issues** occur when it becomes apparent that a security problem exists, was foreseeable or should have been foreseeable and was ignored. Criminal and/or other security problems within your general area (e.g., neighboring parking lots) could be considered advance indicators of security related problems headed toward your facility. Security problems at another JCC or Jewish organization can be considered a substantial indicator.

### Risk Mitigation Analysis

Risk identification is the critical first step of the risk management process. The objective of risk identification is the early and continuous identification of events that, if they occur, will have negative impacts on your operations in achieving their performance objectives or business goals.

There are several ways to conduct risk assessments, and they all begin with compiling information, such as audit reports, security service reports, member complaints, observations, questionnaires, crime prevention analyses (often provided by law enforcement or DHS), an event history at your JCC, information on national issues facing JCCs, reports of local area issues, a professional risk assessment (focused on risk identification and management objectives) and an assignment for your local security committees to identify risk. This manual also includes a security checklist (page ???) that can assist in identifying risk factors at your facility.

Because this process can result in a large amount of data that may or may not be relevant, to start, evaluate each identified issue for further consideration under your risk management program. Issues can be included, excluded and/or put on a future evaluation list. Document and retain all findings. An Excel spreadsheet is often an effective method of organizing and recording this data.

### Distill each finding into a brief summary that includes:

- Descriptions
- Its potential impact to your organization (high, medium or low)
- Your decision on action required (include for action, exclude or retain for future evaluation)
- Prioritization (high, medium or low)
- Associated cost (estimated)
- Permanent mitigating controls, temporary controls and associated costs
- Time frame for completion, including project updates
- Evaluation of completed mitigating controls, further action required (if applicable) and schedule for re-evaluation
A gap analysis can be a useful tool to help in this process. A gap analysis involves the comparison of actual performance against potential or desired performance. It focuses on evaluating existing processes, procedures, functions and systems, and outlines the steps needed to take you to your desired performance level.

**Lessons Learned: Example of a Rear Emergency Door Propped Open**
A rear emergency exit door to the facility is found propped open and, on occasion, persons have been seen entering, exiting and/or granting access to others via this door. For long periods of time, this door has provided access to unauthorized persons.

**POSSIBLE IMPACT**
This risk is high. An unauthorized person could be injured while on-site or harass, abuse, injure or fatally injure staff or members, including children, and/or could steal JCC and/or member assets. This could also damage your reputation, impact enrollment and create an insurance issue.

**DECISION**
Reduce the risk.

**PRIORITIZE**
High priority; this should be one of the first risk-reduction projects.

**PERMANENT MITIGATING CONTROLS**
All fire egress doors should be equipped with a day alarm system that will alert reception, administration and/or security of unauthorized opening of fire egress doors. Consideration should also be given to installing additional cameras to monitor all entrance and exit access points. Alarms and video systems should be constantly monitored; the daily security inspection program should focus particularly on this exposure (signs or indications of doors being propped open and/or alarm systems being tampered with, etc.). A written process should be developed for responding to the unauthorized opening of exterior doors and signage should be installed restricting use to emergency egress only, warning that door opening will result in an alarm condition and a security response.

**TEMPORARY CONTROLS**
Security, maintenance and/or staff should monitor fire egress doors for unauthorized access whenever the facility is open. If staffing is not available, a temporary security guard should be hired until permanent controls can be developed and implemented.

**ASSOCIATED COSTS (ESTIMATED)**
Day alarm system for one access doorway: $350
Video camera system for one doorway: $900

**TIME FRAME**
Day alarm (budgeting, system, vendor selection and installation): 30 days
Video camera (budgeting, system, vendor selection and installation): 45 days

**PROJECT UPDATES**
Project information will be updated after each phase of the process (budgeting, system and vendor selection, installation and system testing). Phases I, II and III have been completed.

**FINAL EVALUATION ON COMPLETION OF MITIGATING CONTROLS**
This control meets our mitigation expectations.

**FURTHER ACTION REQUIRED**
No further action is required at this time.

**SCHEDULED REEVALUATION**
This mitigating control will be added to the daily facility security checklist and reevaluated upon incident and/or quarterly.

To Start You Thinking About Risk Identification
The list below sets out several examples of situations in which unaddressed risk (high and low) could result in dangerous situations, harm to a facility and/or injury to people. Your JCC may already have a history with some of these issues and you may have implemented controls. It is not possible to create a list of all potential risks that should be included in your risk management process.

This list has been prepared for your consideration and expansion.

- Your facility could be vandalized (anti-Semitic graffiti).
- An unauthorized person could utilize your facility (back doors open).
- Property could be stolen (sports equipment, office supplies, member belongings, etc.).
- Financial information and confidential data could be stolen.
- Cyber threats could be directed toward your JCC (phishing emails, missing data, social media threats, theft of computer equipment, social engineering, etc.).
- Negligent hiring could result in a volunteer with a violent criminal record harming a member.
• Unauthorized persons could access your property when the facility is closed and injure themselves in the playground, recreational areas or swimming pools.
• Local teenagers could utilize your property at night (disturbing paraphernalia found).
• Stored pool chemicals could be used to create a dangerous substance.
• Poorly controlled cleaning chemicals could be ingested by a child.
• Members’ cars could be vandalized, broken into or stolen in your parking lot.
• A member could be victimized by a criminal act in your parking lot or on your property.
• A sex offender could take pictures of children at play and/or harass young children on your grounds.
• A workplace violence issue could take place.
• An employee could be involved in a criminal act.
• A domestic or child custody dispute could escalate.
• A criminal could access your facility to escape law enforcement.
• A violent protest could be staged during a controversial special event held on-site.
• Unauthorized persons accessing a summer camp (day or overnight) could injure campers, destroy or steal property, etc.
• A child could go missing during an off-site trip (campers or educational program participants).
• An act of terrorism (a vehicle targeting children at play or persons gathering outside of your facility, etc.) could be perpetrated.

Conclusion

The above process provides a common-sense approach to risk management. Larger national and/or global organizations would use a much more in-depth, systematic approach to risk rating, mitigation and prioritization. These systems typically include computerized programs and mathematical formulas designed to assist large organizations in determining unacceptable levels of risk across their enterprises. JCCs should be able to accomplish this process efficiently and in a timelier fashion with the above strategy.

This section should assist you in identifying your facility’s exposures and help provide a methodology for evaluating them, developing mitigating controls and fostering a rapid decision-making process to address them. In addition, once a proactive risk-management culture is developed, it should enhance your everyday risk-based decision-making process. Remember, the first step and probably the most important is risk identification.

Questions and Calls to Action

1. What is your JCC’s tolerance level for risk? How does that impact security?
2. Based on your event history related to security, which of the six risk types (acceptable, unacceptable, insurable, undetected, ignored or security negligence) are most prevalent? Once identified, where are the underlying issues and how do you plan to address them?
3. What “lessons learned” example do you have at your JCC? Using the risk mitigation analysis checklist, how will it be addressed?
4. What are the 10 most significant risks to your JCC?
SECTION D

SECURITY DESIGN STRATEGIES:

BASELINE PHYSICAL AND ELECTRONIC CONTROLS FOR HIGH-, MEDIUM- AND LOW-RISK SITES
SECTION D. SECURITY DESIGN STRATEGIES: BASELINE PHYSICAL AND ELECTRONIC CONTROLS FOR HIGH-, MEDIUM- AND LOW-RISK SITES

The security concepts and design strategies in this section are critical components in providing a secure environment and balancing security, operational requirements and customer service. A well-thought-out security design will allow you to be prepared for the unexpected and quickly raise or lower your security profile as conditions warrant.

If you are addressing the need for particular security enhancements, overhauling your facility security or building a new facility, an effective security design will:

- Not impede access in or out of the facility
- Allow only authorized persons’ access
- Provide for quick lockdown capabilities
- Allow you to rapidly ratchet your security protocols up or down
- Provide a secure environment for your staff and membership to enjoy your facility
- Deter bad actors from conducting hostile surveillance
- Provide historic information that could be used during an investigation

Whenever security is incorporated early in the design phase of new construction or renovation, the cost of installation will be drastically less, and security will be more effective. When rolled out as part of something new, staff and member participation elements of a security program meet with limited resistance.

The introduction to this manual explained a four-point strategy for approaching security-related issues. Designing or redesigning your facility with this strategy in mind will maximize the benefits of any installation.

A recap of the four points is:

- Look like, and be, a hard target (bad actors will move on and pick another location).
- Install early detection systems to identify bad actors (notify law enforcement before an event).
- Create appropriate response plans and systems (be ready: have a plan and needed equipment).
- Provide safe havens or an escape strategy (be prepared to escape or hunker down).

Risk

To help determine the specifics of your security plan, conduct a study or risk and threat assessment. (If you use a security consultant, review Section K in this document, which relates to hiring a security consultant.) Alternatively, this manual provides information that will assist you in conducting a self-audit. Upon request, local police departments will often assist by conducting crime prevention surveys.

Factors to consider during risk assessment include:

- Local criminal or anti-Semitic activity
- Global security threats against the community
- Staff, membership and children headcount
- Culture of the community and membership
- Geographic location
- Time and distance from law enforcement
- Threats to the organization
- Threats to the nearby community
- Visibility of the facility

This should not be considered a complete list of threat indicators. Many factors, including both global and local threats, global security conditions, U.S. and foreign political environments and issues related to your JCC should also be considered.

Design Concept

Based on reviews of many JCCs, suggested recommendations have been compiled and labeled Levels I, II and III, with I being the most minimal set of recommendations and II and III providing increased levels of protection. All levels will address the fact that the facilities to be protected are Jewish faith-based community centers.

It is possible that you will need to combine components of Levels I, II and III, along with various components not addressed in this manual, to develop a protective strategy for a particular location.
First Steps:

Forced-Entry-Resistant Barriers

The term "forced entry resistant" will be used throughout this section in conjunction with rating perimeter and interior security doors, glass windows or panels, locking systems, door frames and hinges and nearby walls or ceilings. To be considered forced entry resistant, these must, at a minimum, provide a 10-minute barrier against a forced-entry assault against your primary and secondary entrances and safe haven areas. Your design should withstand an attack by one or two individuals with items that can be easily acquired and transported to your site and/or are ready at your location (gun, knife, hammer, tire iron, baseball bat, metal trashcan, landscape boulder, etc.). This will be referred to as the "forced-entry-resistant standard." If law enforcement response is more than 10 minutes away, your facility's resistance time should be increased to allow time for law enforcement's arrival. If your facility is equipped with an exterior door, an interior door and a safe haven area equipped with another secure door, each barrier that meets the forced-entry-resistant standard will add valuable time to your rating strategy. This standard does not address bullet-resistant materials. The intent of this standard is to disallow unauthorized individuals immediate access through a barrier. Some locations and/or areas may require bullet-resistant material. This threat will be addressed later.

Effective Security Programs

Keep in mind that regardless of the amount of physical security equipment and electronic systems you have installed, your security will not be fully optimized if not managed correctly. Appointing a person to be responsible for security management is critical; without the knowledge and ability needed to manage the security function, your program will not be fully effective. Policies and procedures will be required. The key to good security programs is knowing how to fully utilize your electronic systems and physical security controls, along with training, tabletop exercises and security awareness for staff and members.

Level I Recommendations

The results of field security evaluations conducted prior to the creation of this document suggest that very few JCC locations, if any, would optimize security using only the controls from the recommendations in Level I. Level I should be considered minimum security systems and controls.

Physical Security Controls

1.1 All perimeter doors should be equipped with tamper-resistant locks, closing hardware and tamper-resistant door hinges (if hinges are on the unsecured side of the door). If doors are equipped with glass panels, they should be made to meet the forced-entry-resistant standard.

1.2 The main entrance area should be equipped with a second set of interior doors to create a foyer enclosure (this already exists at many JCC locations). The second set of doors should be equipped with tamper-resistant locks, closing hardware and tamper-resistant door hinges. Making the interior foyer, glass and doors meet the forced-entry-resistant standard is recommended.

1.3 Interior doors to secure areas should be equipped with tamper-resistant locks. If hinges are on the unsecured side of the door, closing hardware and tamper-resistant door hinges should be installed. If the door is equipped with a glass panel or adjacent glass panel, it should meet the forced-entry-resistant standard.

1.4 If exterior doors are equipped with either a glass light or a window adjacent to a door, the glass panel should meet the forced-entry-resistant standard.

1.5 Doors to any interior room that may be utilized as a safe haven area during a security emergency or lockdown condition, as well as access doors to childcare areas, should meet the forced-entry-resistant standard. Doors should be capable of being quickly secured from the inside. Door windows or adjacent glass panels should be forced entry resistant and equipped with opaque covers that could be used to cover glass panels during times of lockdown.

1.6 The reception area should be within close proximity (30 feet or less) to access doors and in direct view of the doors. The reception area should be equipped with a telephone, camera monitoring terminal and silent alarm, and have the ability to lock down nearby exterior doors. Computer monitors and/or other possible obstructions should not block the receptionist's view of the main entrances and exits, high-traffic locations and/or sensitive areas.
1.7 If applicable, entry to eateries or stores accessible to the public should not be located beyond JCC security checkpoints. Such facilities should have dedicated exterior entries and exits, with no interior connections into JCC space. The general public should not be granted access to JCC space in order to enter other facilities. Only authorized persons utilizing JCC facilities or JCC tenant facilities should be admitted past JCC checkpoints.

1.8 The exterior of the buildings should be free of decorative foliage and/or debris to allow for quick and efficient inspections.

1.9 Play areas and child pick-up and drop-off areas near roadways must be designed to prevent vehicle and pedestrian crashes (accidental or malicious).

1.10 Playground areas utilized by children participating in daycare, preschool, day camp, etc., should be within an enclosed/fenced-in area. The fence should be high enough (within local code ordinance) to discourage unauthorized removal of children from the exterior side of the fence. The fence should not be near any structures, play equipment, trees, etc. that would aid a child climbing over the fence. Fencing can be equipped with privacy material (highly recommended). To ensure that no unauthorized items are hidden near the fence, decorative foliage should not be planted against the fence.

1.11 Any room or closet utilized to store hazardous materials or chemicals should be equipped with a solid metal door, a tamper-resistant lock and hinges, and an automatic door closer that will automatically relock the door when it is closed. Chemicals should be stored in an appropriate locked cabinet or container that is approved for this type of chemical by local code and/or manufacturer.

1.12 Unprotected exterior utility connections (natural gas, etc.) should not be near roads or driveways. In areas where they are exposed, they should be protected with vehicle barriers, secured where appropriate, within a fenced cage and under video surveillance that utilizes video motion detection.

1.13 If applicable, appropriate "No Trespassing" signage should be utilized.

1.14 If applicable, tenants in leased space should have their own entrance and exit areas. Tenant space should not have direct access to JCC space.

**Systems**

1.15 Access control systems for members should require two levels of authentication: a security token (such as a key fob, access control card or smartphone app) and a current photograph of the member. The front desk and other relevant locations should be equipped with terminals that have access to the member database, including relevant information and a current photograph of each member. A photo and relevant information should be automatically displayed on the reception area terminal when a member presents his or her security token to a reader (exterior door, front desk token reader, turnstile, etc.). Terminals should be positioned so as to avoid displaying confidential membership information in a public area.

1.16 Video intercoms should link exterior access points (main entrance, secondary entrances, loading dock, delivery area, kitchen door, etc.) with reception, security and/or office areas.

1.17 Facilities equipped with a children’s daycare center should also have a video intercom system linking the daycare area and the reception and/or office areas.

1.18 A simple visitor management procedure should be used to record visitors’ names, arrival times, reasons for visiting, destinations and departure times. A review of government ID (such as a driver’s license or passport) should be conducted to verify the identity of the individual. It is recommended the ID be scanned or photocopied for your records. Visitors should be issued a visitor pass. This process should be used for anyone who is not an employee or a member, including consultants, volunteers, construction workers, cleaners, delivery people, tenants’ guests and employees’ visitors. A procedure should be developed to notify any employees or tenants receiving guests before allowing such guests building access.

1.19 Emergency egress doors should be equipped with local alarms that sound when the doors are opened.

1.20 All accessible doors and windows should be protected with a burglar alarm system for when the facility is closed. The system should allow for areas to be closed and locked independently as would complement the operational schedule of your JCC.

1.21 All emergency egress doors should be equipped with a day alarm that sounds at a central location (such as security, reception or administration) and in the immediate area of the door.
1.22 Consider a camera system to monitor the primary entrance, primary exit and main reception area of the facility, along with preschool entrance and reception areas, sensitive locations and a general view of the parking lot. Depending on facility layout and staffing, cameras should be monitored from a minimum of two areas (reception desk, childcare reception, security, office area, executive office space, etc.). All cameras should be digitally recorded with images stored for a minimum of 30 days, record a minimum of 15 frames per second, be equipped with video motion detection capability and a secured IP, and be accessible from local IP and via secured mobile device. All camera views should be adjusted to eliminate unnecessary areas (such as too much ceiling, a blank wall or intense light sources). A policy should be implemented to ensure that video-recorded images are reviewed daily to confirm that cameras are recording appropriately and to determine if any suspicious activity occurred while the facility was closed. All security controls, passwords and/or encryption on individual cameras, networks, routers and storage devices should be appropriately set to protect live or stored images of your facility.

1.23 At a minimum, a facility should be equipped with an audible announcement system to notify staff and members of emergency conditions.

1.24 The exterior of the building (main entrance area, walkways, parking lots, recreational areas, perimeter of the building, etc.) should be well-lit.

Level II Recommendations

Level II recommendations are made with the assumption that all Level I security controls have been evaluated and that selected controls have been implemented. The results of field security evaluations conducted prior to the development of this document suggest that most JCC locations would choose to implement both Level I and Level II recommendations.

The threat of an unauthorized and potentially violent person accessing your facility through your main entrance area is a serious concern. This threat can include a violent situation in front of a facility spilling over into a lobby and possibly throughout a building. Threats can also include a criminal being pursued by law enforcement looking for someplace to hide, a workplace violence event, an emotionally disturbed person accessing your facility or a hostile actor, terrorist or active shooter having access to your facility. Even a thief in your facility who is apprehended by a member could cause a violent encounter. Events of this nature happen quickly, are unpredictable, can happen at any location and can have life-threatening consequences. To limit the ability of an unauthorized and potentially violent individual to covertly or forcefully enter your facility, it is recommended that you consider the following modifications.

Physical Security Controls

2.1 Construct or modify your entryway to include an exterior door and interior door, with a foyer area in between. Both doors should meet the forced-entry-resistant standard. (Many JCCs’ entrance areas are configured in this way, but they are not forced entry resistant.) The foyer walls or ceiling may be made of glass. This design is open and provides an unobstructed view of the entranceway. It is recommended that one side of the foyer be utilized for entrance and the other for exit, with a forced-entry-resistant wall separating the two sides. This will provide added security if someone tries to push through an open exterior door.

The primary difference between the type of entryway described above and the one referred to in the Level I section is that the Level II entrance will be made to meet the forced-entry-resistant standard. Forced-entry-resistant modifications should be undetectable. Controls of the interlocking doors can be operable in many ways depending on the time of day, current threat level, available security, etc. An emergency lockdown system should be able to lock down all doors, or just the exterior or interior doors, depending on the nature of the current threat.

Typical applications of this equipment:

A. Exterior front door locked. Access is granted via access control token or video intercom to reception/security to release lock.

B. Exterior front door locked. Use of access control token will bring up system photo of arriving member, receptionist will evaluate photo and arriving guests and provide access as deemed appropriate.

C. Exterior door unlocked and interior door locked. Access is granted via access control token, video intercom to reception, monitoring camera system or within view of receptionist.

D. Both exterior and interior doors locked. This could also be used as a “mantrap” that would not allow the inner door to open until the exterior door is closed; only authorized people are in the foyer or between the doors, which are unlocked independently. One of the abovementioned controls can be utilized for manual operation of doors.
E. In addition, the following systems and controls can be modified (all doors locked, outer or inner doors locked or unlocked, etc.) when warranted by security conditions and/or business needs. Additional security staffing (recommended) may be required when all doors are unlocked, which might happen during large-scale events.

2.2 An unsuccessful attempt to smash through your main or secondary entrance area could drive an unsuccessful intruder to attempt to access your facility through a nearby window or door. It is recommended that windows and doors located near main access doors be made forced entry resistant. This can be accomplished by applying a security film to existing glass, anchoring the frame to the existing frame or anchoring new laminated security glass to existing frames. Frames must be evaluated to determine whether they are strong enough to withstand an attack. The exact distance from main doorways to windows and nearby doors at risk will depend on several local factors and conditions. At a minimum, without additional considerations, it is recommended that windows and doors less than 100 feet from the entrance be made forced-entry resistant.

2.3 Secondary staff and member entrance areas and exits should have the same level of security controls (physical, electronic and staffing) as described above for the main exterior entrance.

2.4 Installing appropriately placed turnstiles at your member entrance areas will help allow access only to those who are authorized to enter the facility. They will act as a strong deterrent against anyone who might try to sneak in when your reception area is active. However, turnstiles are not generally considered to be forced-entry-resistant barriers. There are many types of turnstiles, from standard metal-arm turnstiles to full-height units. Turnstiles can be designed with glass barriers that retract or have optical systems with no barriers. They can sound an alarm, flash a light and/or close the gate when someone does not use an active token before stepping down the turnstile alley. The size of the reception area, peak traffic times, staffing and local building codes will affect which type of turnstile is chosen and where it is located.

2.5 If an unmanned access door is required, it is recommended that a single-occupancy access control point be used. A revolving security door can be used, which will permit only one occupant at a time to enter or exit the facility. Entry can be controlled via video intercom and two cameras nearby the entrance. Reception can verify arriving staff or members and provide access. Exit from the building will be unrestricted. Do not use this type of access point for guests or other individuals unknown to the JCC. Consult local building codes.

2.6 The facility’s delivery area should be designed with a solid metal roll-up gate and a forced-entry-resistant exterior door. Access doors that connect the delivery area to other parts of the facility should be forced entry resistant and have access control from both sides of the door.

2.7 Emergency egress doors should only be utilized for emergency egress.

2.8 Limited-use doors (such as kitchen, backstage or building engineering doors) should be forced entry resistant, access controlled from both sides (if permitted by local fire code) and monitored via camera system. Access through these doors should be restricted to authorized users.

2.9 Exterior windows in rooms where confidential activities or events for children take place should be made opaque from the exterior and clear from the inside out.

2.10 The appropriate level of security for exterior access doors that lead to playground areas, swimming pools and ball fields will require a site-by-site security evaluation. Leaving these open and unattended can provide easy and undetected ways to access your facility. At a minimum, this type of access point would require staffing by a security person when doors are unlocked, and the general area must be monitored by your camera system.

2.11 Doors accessing childcare areas and/or classrooms should be made forced entry resistant.

2.12 Fencing of recreational areas with direct access to facility entrances and exits will improve security within the boundary of the fence and coverage of access points into the facility. It is recommended that a security-grade fence (six feet high with anti-climbing fabric) be installed around the perimeter of recreational areas directly connected to the facility (such as swimming pools, playgrounds or ball fields). (Note that the height of the fence and the number of gates/doors will be dependent on local building codes.) Fence installation should clear structures and trees that would aid in the climbing of the fence. All fence emergency exits should be equipped with an alarm sensor to indicate if the fence gate has been opened, a local sounder at the fence and annunciation at security or the reception desk. This area should also be monitored by your camera surveillance system. Any facility door utilized to access a fenced area from a building should be included in your emergency lockdown system. If access is permitted via a
fence entrance, it should be equipped with all the relevant security equipment securing your main reception area.

2.13 The forced-entry-resistant standard applied to rooms and areas chosen to be safe haven locations should include accessible walls, ceilings and floors. Exterior windows in safe haven locations should be capable of preventing viewing from the outside. This can be accomplished with an opaque window treatment pulled into place during a lockdown.

2.14 Under Level II, consider the use of security guards for security-related duties in reception areas and for internal and external inspections and patrols. These guards should not have reception duties.

Electronic Security Controls

2.15 Consider camera coverage above that suggested in Level I to provide a higher level of surveillance. Key enhancements would include equipment to detect hostile surveillance, suspicious behavior, anti-Semitic tagging or activity and criminal acts. This system should be able to detect suspicious activity and provide a usable, high-quality image of unauthorized individuals in key places on your property. Consider cameras that capture the following:
   A. Clear pictures of arriving staff, guests and members at the main entrance, turnstiles, loading dock, kitchen delivery door, entrance to pool area, etc.
   B. All facility entrances and exits
   C. Main corridors leading to and from reception, office areas and other high-occupancy areas
   D. Secluded areas of the exterior of the building
   E. Wide view of exterior play areas
   F. Chemical storage areas
   G. Building utility access points
   H. Garbage collection areas

2.16 All vehicle entrance areas (members, staff, delivery, etc.) from public streets to private property should be considered for additional cameras. Cameras clearly capture high-quality images of license plate numbers and vehicle occupants.

2.17 Any locations determined to be important in the management of a community center should be monitored by cameras.

2.18 A professional electronic access control system that can distinguish between employees and members should be considered. It should also be capable of integration with your video control and recording equipment. There are many types of access control tokens, including cards, fobs and smartphone apps. Access control systems have many useful features (anti-pass back controls, “door held open” alarms, one-button lockdown, unauthorized access, activity reports, etc.) that can be automatically programmed to provide a safer environment. All of these features should be evaluated.

2.19 To act as a deterrent and to provide emergency assistance to staff and members in your parking lots and in exterior play areas, a blue-light call box (duress alarm system) with intercom and video monitoring capability should be considered.

Level III Recommendations

Level III recommendations are made with the assumption that all Level I and II security controls have been evaluated and selected controls have been implemented. Field security evaluations conducted prior to the development of this document suggest that several JCC locations would choose to implement Level III recommendations or a combination of components from all three categories.

Level III locations are at a higher risk of being attacked. As discussed in earlier portions of this manual, quick identification of suspicious behavior, suspicious conditions and/or a hostile act is critical, as is a quick response time. All of the recommendations are focused on identifying and delaying a hostile actor.

Once it has been established that your facility is at higher risk, prompt and appropriate actions must be taken, which include providing a safe environment for employees and members (lockdown and move to a safe haven area) and invoking a quick response by law enforcement and/or your own response team. This section will discuss several advanced mitigation strategies and equipment that will provide some guidance to help you evaluate options. Due to the complexity of today’s threats, the technologies to address them and the variation in JCC facilities’ designs and operations, a security professional should review and approve your plans prior to implementation.

3.1 At this level, a dedicated security director should be appointed to oversee your security program. Please refer to Section K, which covers hiring a security director, to help you develop the role and its responsibilities. This section will also assist you in identifying a qualified candidate or appointing an existing staff member.

3.2 All ground floor or accessible windows should meet the forced-entry-resistant standard. Consider applying bullet-resistant material to publicly exposed areas, main entrance areas or windows into sensitive areas. When considering bullet-resistant material, note that weapon types and
bullet calibers will determine abilities to penetrate bullet-resistant material. Practically speaking, nothing is bulletproof. However, it is difficult to accurately aim a weapon if the shooter cannot see his target. In high-risk areas, in addition to bullet-resistant material, consider making glass partitions opaque. This could be accomplished by permanently installing opaque material or by using a temporary window treatment during high-risk hours and events.

3.3 To provide additional protection for reception staff, the reception area should be enclosed and made to meet the forced-entry-resistant standard. Where threat levels are higher, consider applying bullet-resistant material.

3.4 Doors leading away from reception areas should meet the forced-entry-resistant standard and should be capable of electronic lockdown from the reception and office areas.

3.5 When establishing safe haven areas, choose locations with exterior and interior windows.

3.6 Consider a vehicle arrest system to prevent a hostile actor from utilizing a vehicle to damage the building and/or harm individuals near the building perimeter and individuals in exterior play areas. Vehicle arrest systems can be either man-made or part of your natural terrain. Man-made vehicle arrest systems are engineered according to your threat level, the type of vehicle and its anticipated weight, distance to impact, potential speed obtained and driver intent (to deliver a harmful device or use the vehicle as a weapon). This would require a vehicle impact study. The U.S. Department of State tests and certifies vehicle arrest systems to ensure their effectiveness. Natural terrain (such as a curve in the road) can impact a vehicle’s speed and ability to cross certain natural barriers. Examples of natural barriers include a raised terrace (approximately four-foot vertical height), mature trees, large and heavy stone boulders, depressions in the ground, water, etc. Natural barriers can be enhanced with architectural components and reinforced masonry walls. Whatever type of barrier you utilize, place it as far away from the protected area as possible. Without factoring in the intent of the driver (to deliver an explosive device, ram pedestrians, fire weapons, use edge weapons, etc.), generally the more distance from an intended target, the more effective a barrier system will be. Distance is critical when limiting a vehicle with explosive cargo. There are also temporary controls, such as a dump truck filled with sand, a large bus, construction equipment and/or Jersey barriers, which can be utilized when a threat level rises rapidly and there is no time to develop and install a permanent solution. In addition to temporary barriers, armed security or police personnel can also provide an effective deterrent or response to an active threat.

3.7 Consider installing a full perimeter fence. A fence will act as a deterrent, allow you to quickly identify an unauthorized person climbing over and/or tampering with the fence and provide you additional time to notify police and lock down your facility. The fence should be a minimum of six feet high and equipped with anti-climbing fabric or construction concepts. Local building and fire egress codes could mandate the fence height, location, number and type of gates (emergency egress) and other aspects of construction. Regardless of the ground’s terrain, there should not be more than one inch between the bottom of the fence fabric and the ground. When planning fencing, it is important to remember that fencing should not run near structures and/or foliage that will assist in climbing the fence. Do not place fencing directly against dense foliage that will block your ability to monitor the fence and provide a place to hide destructive materials. If possible, keep a minimum of 10 feet clear on the exterior side of the fence to assist in identifying individuals tampering with and/or preparing to climb the fence.

3.8 To limit unauthorized vehicle access to JCC property, consider establishing a security checkpoint at your main and secondary vehicle entrance areas. Traffic should be controlled via mechanical gates (entrance and exit) and security guard booths that are staffed during operating hours. Security guard booths should be equipped with communications equipment and provide the ability to view cameras relative to their assignments and responsibilities. The security booth areas should be protected against accidental and/or malicious vehicle collisions. If high threat conditions warrant the use of bullet-resistant glass and partitions (walls, doors, windows, etc.), security booths should be fabricated and/or modified to be bullet resistant. The bullet-resistance level should be dependent on a threat assessment of current conditions at the time of design.

It is highly likely that a Level III operation will require a security guard force (proprietary, external or a combination of both) to operate efficiently. There is definitely value in having an on-site response team. It could limit the effects of a bad actor and/or act as a deterrent. This is not a question that can be answered without a detailed analysis of your individual location and threat conditions. A temporary solution to a rapidly evolving threat could
be to hire off-duty law enforcement guards until a full analysis can be conducted and permanent mitigating controls can be developed and implemented.

Security guards can be deployed at the primary vehicle entrance, conduct roving patrols (internal and external), be stationed at primary entrances and exits, staff high-volume arrival and departure times, manage traffic and have the ability to respond to emergencies.

With respect to the question of armed or unarmed security guards, take these considerations into account:

- Will the security guards be employees or external subcontractors?
- Will they have the appropriate training and experience, as well as continuous certification regarding shooting skills?
- Will they meet reasonable health and fitness requirements?
- What is their policy on the use of deadly force?
- Will weapons be visible?
- Will your membership appreciate their presence?
- Will the security guards receive ongoing training?
- Will they have the appropriate level of insurance? If they are internal, will your JCC have the appropriate level of insurance?
- If you have a security director, will that individual be armed? Is the individual a retired law enforcement guard? Is he carrying his weapon at your request? (This would require additional insurance and may leave you open to legal issues.)
- Does your site have a no-weapons policy for general staff and membership?

Having an armed security detail is only one aspect of a security management program. It does not replace all of the abovementioned controls. All too often, having a single armed security guard on-site is erroneously considered to be the solution to a long-term problem. The best solution is to have an integrated approach to protection management that combines electronic and physical security controls, security policies and emergency management procedures and integrates armed security personnel. This is not a straightforward issue, and it should be addressed on a case-by-case basis.

**Systems**

**3.9** To provide a better early warning system, your video camera and monitoring system should be enhanced. Additional cameras could cover remote areas of the building or buildings, both sides of entrance and exit doors, any high-risk areas, exterior property entrances, fence lines, exterior recreational areas, approaching roads and other key areas unique to your location. A central monitoring location should be established. Monitoring equipment should include large-screen monitors that display sensitive areas as well as video motion alarm activation. Suggested locations for this monitoring station could include the reception area, a security desk, an office area or a security guard booth. The station should be manned at all times. Secondary monitoring locations should also be considered for any of the above-mentioned areas. This will provide a more flexible way of monitoring your system. Considerations for staffing should include the current threat level, local conditions, the day’s activity and the time of day.

**3.10** Access control systems can be expanded to include additional doors and areas to provide a higher level of security and accountability.

**3.11** Many additional electronic security components can augment your security systems. These additional components include metal detection portals, mail scanning equipment, license plate readers, fence alarms, gym bag scanning equipment, facial recognition, movable vehicle bollards, wireless access-control tokens, exterior security drone patrols, biometric access-control equipment and much more. Evaluate this type of equipment to determine how it would assist in mitigating exposures and how it would be integrated into your staff and membership culture and environment.

**3.12** Because many of the above security enhancements will help to keep out bad actors, note that in certain circumstances they could impede law enforcement’s progress in reaching an event on your premises. Most law enforcement departments are prepared to meet this challenge. If your location implements the forced-entry-resistant standard with bullet-resistant partitions, incorporate an unlock feature. This feature should be controlled on-site and/or remotely. It can be as simple as having keys readily available.

**Childcare Programs**

JCCs operate numerous early childhood programs. For areas where early childhood programs are held, including early childhood rooms, gymnasiums, studios, theaters and playgrounds, it is prudent to consider security enhancements beyond those set out above. In all early childhood areas, follow the forced-entry-resistant standard for windows and doors and the above safe-haven guidelines.
Conclusion

Businesses that are open to the general public cannot avoid addressing threats. In today’s world, where there is no rhyme or reason as to where the next hate crime or act of violence will occur, your security posture must be designed to prevent an event from occurring at your location. Given the quantity of services you provide, including events and services for children, the number of your participants and on-site tenants and the sometimes multimillion-dollar value of your facility and assets, many JCCs operate like thriving corporations. Not many years ago, the level of security discussed within this document would have been considered excessive. When thinking about your new security posture, you should consider your JCC not only as a community center, but also as a vibrant business.

The primary objective of this document is to assist you in allowing only authorized persons into your facility, being prepared to respond to emergencies and adjusting your security posture according to current threats. There is no one silver bullet or single piece of electronic equipment that can do the job. Senior management participation as well as carefully designed policies and procedures are needed to shape systems and provide a safe environment. Security is a matter of integrating technology, management, emergency response, awareness and operational procedures.

Security Sometimes Fails for Simple Reasons

- Systems have not been tested. A malfunctioning device goes unnoticed, or it is noticed but not repaired in a timely fashion.
- Relevant individuals do not know how to fully utilize systems and controls or are not reviewing yesterday’s video footage.
- A back door is left open for ventilation (sometimes bypassed in your alarm system), allowing an intruder to gain undetected access to your facility.
- A gate in your fence line is left unlocked so staff can quickly get to their vehicles or provide access to friends.
- Security staff lacks the necessary training to interpret a suspicious act, or a suspicious act goes undetected.

You must address issues both major and minor on an ongoing basis. You should regularly conduct audits, evaluate staff, conduct ongoing training and review procedures. Good security practices closely resemble good business practices.

Questions and Calls to Action

1. Is there a staff member at the JCC whose full or partial responsibility is security? If not, what plans are there to incorporate that function within the organizational chart?
2. Based on a review of the three levels of recommendations for security design, where is your JCC currently?
3. What additional elements of security design are needed immediately, in the short term and for the long term?
4. How often is equipment associated with security checked, repaired and upgraded?
5. Is security design incorporated into the planning of JCC activities?
SECTION E

CRISIS MANAGEMENT STRATEGIES AND PROTOCOLS
SECTION E.
CRISIS MANAGEMENT STRATEGIES AND PROTOCOLS

By definition, an emergency is an unexpected and unpredictable event, and a crisis is an emergency that has reached a critical phase. For purposes of this manual, we will distinguish an emergency from a crisis based upon how severely an event will affect the institution experiencing it.

Generally, security crises fall into two categories: poorly handled or overwhelming emergencies that quickly turn into crises, and events that are crises from the moment of inception, due to their nature. There are several ways to lessen the impact of a crisis on your organization. Advance planning and training prior to an event are two of your biggest advantages.

The Event
The time between the start of the event and its conclusion is the focus of your crisis management program. The amount of time between “just another day” becoming an emergency, and then a crisis, can be short. Based on conditions and circumstances, your participation in an event can last anywhere from a few minutes and several hours. In some types of crises, your role could end as soon as law enforcement arrives. In other types of crises, such as those in which a crime has not yet been committed or a crime committed is not yet of a threatening nature, your participation will be ongoing.

Crisis Management Mode
Once in crisis management mode, you and your team will become incident commander and emergency response team. Every second will count. As soon you OBSERVE the situation, you must ORIENT yourself, DECIDE on next steps and take ACTION (“OODA”). The more quickly you do this, the more effective your response will be in minimizing the event. The OODA decision-making strategy will be discussed further later in this section.

In some types of emergencies or crises, you will have time to customize and refine your response. These could include a hurricane, a snowstorm, flooding, a planned protest, etc. You will not have time to develop a plan, but you may have time to enhance and customize an existing emergency response plan to address the situation at hand.

All parties at JCC locations should recognize that first responders and emergency personnel may respond differently to particular situations (medical emergency, vehicular accident, terrorist attack, fire, bomb threat, etc.) based on their professional training and as directed by their superiors. Arrival times of first responders can vary greatly. Relying solely on first responders is not a crisis management plan. In some types of events, first responders will take complete and total control (fire, crime, mass medical event, etc.) and in other instances, they might look to your organization for direction.

Strategy
Some say you can’t prepare for everything. This may be true. However, for some, this is a justification for failing to prioritize crisis management preparation, emergency preparedness training, and the integration of risk-based decision-making into overall business plans.

Training is crucial. The American Red Cross states that organizations that have prepared for a crisis do better than those that have not prepared. This holds true even if the organization was prepared for a tornado but instead had to respond to a terrorist attack. Training in the basics of crisis management (finding shelter, protecting yourself and others, staying calm, being observant, moving away from the event, providing leadership, etc.) can be helpful in many types of emergencies and crises.

Archilochus is said to have written: “We don’t rise to the level of our expectations; we fall to the level of our training.” A popular quote among Navy SEALs is very similar: “Under pressure, you don't rise to the occasion; you sink to the level of your training.” Both quotes emphasize the need for training. We may not be able to avoid or neutralize every crisis, but if we prepare and train, we can sometimes dramatically affect the outcome and impact of an event.

Proactive participation is another key factor. Promoting ongoing awareness and a culture of identifying, reporting and quickly eliminating exposures will help limit emergencies and crises.

Planning and training can minimize emergencies and crises. Integrating security and safety objectives into current and future processes, procedures and projects will limit and manage your organization’s critical events.

Preparing to Develop Your Plan
The primary reasons why security systems and controls fail are discussed in several chapters throughout this manual. They include ignoring known conditions, unrecognized security and safety exposures, a lack of planning
and a slow response to critical issues. Reviewing other sections of the manual will help you proactively identify critical processes, recognize security and safety issues, encourage staff and members to report issues to management and develop and design new projects and procedures that will inherently limit risk.

**Review the following sections:**
- Introduction (Section A)
- Security and Safety Awareness (Section B)
- Risk Management (Section C)
- Site Inspections (Section H)
- Security Committee (Section I)

Your first objectives are to create a list of possible emergencies and/or crises; develop your crisis management strategy; implement recommended policies, procedures and/or controls and conduct training (lectures, tabletop exercises, drills, etc.).

A plan should encompass potential responses to critical events (suspicious person or package, bomb threat, act of violence, hurricane, medical emergency, etc.) as well as training and drilling. Once your plan is in place, the crisis management team should continue to collect, analyze and maintain information gathered, brief members on local issues and update the plan as necessary. The objective of a JCC crisis management team is to determine the steps necessary to safely come to a positive conclusion to a negative situation.

**Crisis Management Team Concepts**

The crisis management team should consist of staff members whose collective oversight covers each of your JCC departments. In some JCCs, partner organizations should be briefed on all emergencies and crisis management plans. In some cases, they should have representatives on the team. If the JCC is not the primary organization responsible for security (as on a campus), a senior manager should represent JCC interests on the campus crisis management team.

Each team member will be responsible for administrative issues, gathering information and presenting critical issues. The director of the team should be the CEO/executive director or his/her designee. In some organizations or under certain circumstances, the CEO/executive director may be otherwise focused on matters relating to the crisis or other pressing issues. Depending on circumstances, the CEO/executive director would either sit on the team or receive updates from the team director. Each individual who sits on the team should have at least one deputy should he or she become unavailable.

**The crisis management team has three operating modes:**

1. Normal Mode, in which team members attend scheduled meetings to exchange information and review and revise the crisis management plan.
2. Response Mode, in which team members convene to analyze dangerous conditions, suspicious or threatening information and new threats and concerns (such as a hurricane, a bomb threat or a planned protest) and make prompt decisions.
3. Implementation Mode, in which the crisis management plan is put into immediate effect in response to a hostile act (e.g., an active shooter). In this mode, you rely on planning and trained staff, which is why planning, training, drills and tabletop exercises are critical. Some features of this mode include:
   - There is no time to convene a meeting.
   - It is critical that at all times someone on-site is empowered to make announcements, call police, provide direction, work with local law enforcement and make emergency decisions.
   - With very little information, this person must make best-case-scenario decisions and provide the safest environment possible.

**Ongoing**

The crisis management team should meet at least once each month. During each meeting, the director of the team should prepare a brief summary including open issues, recent activity, pending threats and changes or enhancements to the security program. Each meeting should also feature a brief exercise or discussion concerning a possible threat and the appropriate responses. Keep minutes of each meeting. After the program has matured, scheduled meetings can be held quarterly.

**Crisis Management Center**

Establish two local crisis management centers—a primary center and an alternate. A centralized point of operation is necessary for successfully managing crises and emergency conditions. All senior management and staff will know where to report and where they can receive critical information. If your primary crisis management center is unavailable, senior management and staff should automatically go to the secondary location.

Any room that will accommodate your team as it conducts business can serve as a crisis management center. It does not have to be a dedicated room. A conference room that can quickly and comfortably accommodate all team members and the required supplies and equipment would suffice. Avoid rooms in the basement or on street level.
Basic requirements for a crisis management center include: generator power, a direct copper telephone line, a basic analog telephone, network capability for the required number of PCs or laptops, access to cable network news, a TV monitor, two-way radios, a basic first aid kit, a defibrillator, cell phone charging equipment, flashlights, batteries, drinking water, nonperishable food, contact information for all critical staff and members, and paper and digital copies of your crisis management plan and vendor information. A storage closet in the vicinity that has sturdy walls, doors and locks should be dedicated to emergency supplies. Audit supplies and room fitness each month, and test equipment every 90 days and whenever construction or maintenance work could impact the copper cable, generator connections, network connections or installed infrastructure components.

The primary and secondary crisis management should be equipped equally.

You should establish a virtual crisis management center as well. This can simply be a prearranged conference bridge enabling senior management team members to communicate prior to the physical centers becoming operational or when conditions do not permit access to the either the primary or secondary centers.

In addition, designate an off-site crisis management center where in-person meetings can take place in the event that your facility becomes unavailable. This should be a location that can accommodate your team, serve as a staff assembly area and allow you to conduct business temporarily. You could choose a nearby hotel, school or associated facility. Depending on your threat level, you could store some communications and computer equipment at the off-site crisis management center. In lower-threat environments, each participant would be required to bring his or her own communications and computer equipment. During off-site crisis management conditions, it is also critical to have all the necessary information on hand to develop crisis and recovery operational plans, including paper and electronic copies of all critical information needed to conduct business off-site for a minimum of 30 days.

Roles and Responsibilities

Each person on the crisis management team should have clearly defined areas of responsibility and authority. Decide who has authority to declare a crisis and make decisions, and designate deputies to do so in their absence. Whenever the facility is operational, someone on-site must have this authority.

Develop guidelines for activating your team and/or declaring a crisis.

Once a crisis has been declared, all of the crisis management team members should be immediately notified using the best means of communication available. Depending on the type of crisis (personnel, medical, natural disaster, security etc.), not all members will be required to participate in all aspects of the event. The CEO/executive director should decide who participates.

After initial notification, the crisis management team director must set the frequency and method of communication until the crisis management center becomes operational. Generally, during the initial stages of a crisis, updates should go out every one to four hours, and then be adjusted as conditions warrant. Remember that a crisis event could start in the middle of the day, in the early morning, in the evening or in the middle of the night. Your team must be prepared to communicate and take action whenever a crisis occurs.

When a crisis occurs, conduct an immediate assessment of conditions to determine the impact on your organization, staff, members, tenants (where applicable) and assets. This should be immediately facilitated both remotely and via on-site inspections, if conditions are safe enough. Persons conducting on-site inspections should have the organizational knowledge and expertise to evaluate conditions and impact. Persons gathering information remotely should rely on local government, law enforcement contacts, key persons in the community, similar organizations and the media. Both remote and on-site teams must immediately report any pertinent information to the crisis management team. On-site assessment teams must report their personal status conditions at a minimum of every hour.

Once the crisis has concluded, the crisis management team may need to transition to a business continuation model.

Operational Guidelines

Appoint a crisis management team consisting of senior leaders within each of your organization’s business areas. Each team member should designate a deputy to function in his or her capacity should he or she become unavailable. Team members should draft emergency plans for their relevant business groups and submit them for the team’s review and approval.

Appoint a director of the team, as well as a deputy director. The director is responsible for maintaining the team’s readiness on a daily basis, gathering and coordinating information and presenting critical information to the team and CEO/executive director. The director also has overall responsibility for managing the crisis management program and should be capable of declaring a crisis.
Assign a primary and secondary staff member the daily responsibilities of monitoring conditions that could affect your JCC’s operations. Such conditions could include reported exposures, union disruptions (transportation, sanitation, utilities, etc.), future weather forecasts, planned demonstrations, lost children, sexual harassment, child endangerment, the threat of terrorist activity and/or pandemic or contagious disease outbreak. Monitoring includes reviewing internal reports, observations, media information, law enforcement information, daily security inspections, and more. This staff member should report any relevant information to the team director for further analysis and/or dissemination to the team.

Appoint a primary and secondary staff member to monitor general staff safety and security issues during a crisis and to provide needed resources to staff members. This position should report to one of the senior team members. The roles and responsibilities for this position should include organizing staff transportation, securing food and water, locating accommodations (including overnight housing as needed) and coordinating security throughout the duration of the crisis.

Each site (camp or JCC facility) should appoint a primary and secondary person who will report to the team and be responsible for local management, security, exchange of critical information with the team and execution of team directives.

Depending on the size of the team, appoint two or three assistants to conduct research, draft documents, coordinate transportation and deliveries, record meeting notes and provide general assistance to team members. During non-emergency times, these assistants should also be responsible for maintaining lists with critical information. At a minimum, this should include contact information for staff, vendors, volunteers and members. Contact information for city, state, and federal agencies should also be kept up to date and readily accessible.

In addition, all critical information to manage a crisis and/or facilitate recovery efforts should be identified and made available during an on-site crisis. Store a copy of this information in a secure, off-site location to ensure that it is available if required. Keep all information current.

Once you have chosen your team members, hold at least one full-team meeting to discuss and finalize the proposed structure of the crisis management plan, develop a plan for training, modify operational guidelines as needed, establish areas of responsibility and develop a list of team members authorized to declare a crisis.

Once the crisis management plan has been finalized and all team positions filled, present a training session lasting at least three hours to all team members. The session should address all team members’ roles and responsibilities and provide them with the necessary tools and knowledge to assist in developing plans, identifying exposures, analyzing findings and executing their jobs during a crisis.

Following this training, conduct a four-hour tabletop exercise. This would include three scenario-driven exercises requiring participants to respond as they would during a crisis. Keep these exercises as realistic as possible to forge team members’ ability to work together under duress and provide confidence that the team can manage a crisis successfully. Once the exercise is complete, evaluate its success to refine responsibilities and provide additional training as required.

Any member of the team who becomes aware of information that could adversely impact your operations should immediately report it to the director of the team for further analysis and dissemination. If the information is actionable, all members should be made aware of the issue. If the information is not actionable and does not pose an imminent threat, it should be reported to the entire team during its next monthly meeting.

Whenever actionable information is identified, the team must be notified of pending exposures. All credible information should be taken seriously until proven otherwise. Depending on the nature of the crisis, time of day and day of week, an emergency session should be conducted. This first session can be via a conference bridge for some or all participants or at the primary crisis management center. At this point, develop a timeline tracking the pending threat. For example, a pending threat that is 36 hours from impact (such as a plan to protest or bad weather conditions) might require a minimum of two updates on the first day, four updates on the second day and updates every two hours on the day of the event. You may need to modify this depending on the threat.

At this time, all team members should update and review all data. Persons with responsibilities outlined above should start to execute their areas of responsibility. Check all supplies and equipment relating to the two crisis management centers for fitness. Relocate all mobile or movable assets in the path of the identified threat to safer areas.

All applicable notifications and actions should be reviewed, ready and implemented as individual plans require.

Upon notification, each team member must brief his or her staff on their areas of responsibility. Depending on the threat type, this may mean reviewing their plans, checking their emergency supplies, updating and printing critical information and preparing staff coverage.
The primary crisis management center should be set up, tested and readied for use within a minimum of 24 hours before scheduled impact. At the same time, the secondary center should be readied to stand by if the primary center becomes unavailable. Check all equipment for availability and fitness and correct any deficiencies.

Depending on the crisis type, conduct a review of your off-site crisis management center.

A long-range crisis may be averted at the last minute. However, this does not indicate that all of your preparations were unnecessary or that you should fail to prepare next time. Consider it a training exercise. Never ignore an issue that may have adverse effects on your organization. Waiting for the last minute to set up your crisis management center and prepare your staff will drastically limit the effectiveness of your response capabilities.

If your organization is struck by a crisis without warning, you must immediately switch to crisis management mode. Gather your team in your primary, secondary or off-site crisis management center and initiate a telephone conference bridge for those who are unable to attend in person. You must begin to evaluate the problem, identify impact on your organization, communicate with your staff and start to address each issue. The only difference at this time is that you did not have 24-hour notice to prepare the center, review your plan and/or position staff. Decision-making under crisis conditions can be very stressful. The more time and energy you put into finalizing the plan, preparing relevant documents, delegating responsibilities and training, the easier it will be to successfully execute your crisis management strategy.

Conclusion

A strategy for making critical decisions is paramount. Colonel John Boyd developed a proven concept for making rapid and appropriate decisions during crises to assist pilots in responding to enemy aircraft. It includes a rapid process to Observe, Orientate, Decide and Act (OODA). This concept has been utilized by law enforcement and business organizations around the world. Time between observation and action is the key to limiting exposure to risk. This concept should be the cornerstone of your crisis management program.

Developing an ongoing staff emergency and crisis management training program is as essential as outlining your crisis management strategy. This type of program should include all staff members and long-term volunteers. The training should prepare them to meet your expectations of them during an event. As an added benefit to staff, it should include guidelines for developing a personal plan for themselves and their family members.

When developing your crisis management strategies, be sure to include all relevant exposures to JCCs in general, geographic issues, and exposures in your community and neighboring businesses or industries that could have a negative impact on your organization. As an example, you may not naturally think to develop a response to a chemical spill because there are no factories in your area. However, if you are close to railroad tracks (within a quarter-mile), you should determine if they are passenger and/or commercial tracks and plan appropriately.

Questions and Calls to Action

1. In crisis management mode, who is the crisis management team director, and who makes up the team?

2. Where are the JCC’s primary and secondary crisis management centers. How will you communicate virtually if required? Where is an off-site center located?

3. Under what circumstances would you declare a crisis and activate the team?
SECTION F

SECURITY ESCALATION PLAN
SECTION F. SECURITY ESCALATION PLAN

A security escalation plan does not take the place of a crisis and risk management plan. Having a security escalation plan, accompanied by continual training and drills, promotes a quick and appropriate response by management in order to minimize the impact of an event on your JCC. This section examines six indicators that should cause you to consider escalating security. After you review them, make any adjustments necessary to address implications for your specific geographic location and unique security conditions.

Advantages
Developing a security escalation protocol for your JCC will assist you in implementing an action plan more quickly and efficiently. This approach has two primary advantages. First, it allows you to develop a logical and strategic plan for a security issue before it occurs, without the distractions of limited time, heightened emotion and stress. Second, should an event occur, you will have a pre-approved action plan ready at your fingertips.

The escalation protocol is based your geographic location and the nature of the threats you face, which can include anti-Semitic activity, terrorism and many other security threats that could impact your JCC. No list can take into consideration all possible threats and mitigating controls. The primary intention of this document is to help you prepare for different types of threats and to be ready to respond quickly and effectively. This type of strategy can be utilized for a number of different types of emergencies (wildfires, crime, chemical spills, floods, epidemics, etc.).

Six Indicators That Should Cause You to Consider Escalating Security
- Global threats to Jewish organizations
- Nationwide threats to Jewish organizations
- Statewide threats to Jewish organizations
- Statewide threats to similar types of organizations
- Local threats to Jewish organizations
- Specific threats to your JCC
**Escalation Strategy Checklist**

Utilizing the strategy below will help you balance security and operational needs while rapidly responding to threats. No single document can address all possible situations that can arise.

This checklist is most effective when tailored to your individual JCC. Each of the categories in this list will assist you in creating an escalation strategy suited to your environment.

Each category of this checklist can function independently. For example, if there is a statewide threat to Jewish organizations, you can refer directly to the 3rd checklist category. When developing a strategy for a particular threat, you may need to incorporate controls from other categories to provide a balanced approach.

As domestic and international threats continue to evolve, continue to review and update your escalation strategy.

### 1. In the Event of a Global Threat to Jewish Organizations

<table>
<thead>
<tr>
<th></th>
<th>Recommended Escalation Protocol:</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>1.1  Crisis management team should evaluate the potential threat level to your organization and allocate resources if required. Meeting of the crisis management team and security committee.</td>
</tr>
<tr>
<td></td>
<td>1.2  Crisis management team should assign an individual to monitor global threats to determine if they could impact U.S. JCCs. This person should provide daily updates to the crisis management team.</td>
</tr>
<tr>
<td></td>
<td>1.3  Conduct a basic review of all security and crisis management planning.</td>
</tr>
</tbody>
</table>

### 2. In the Event of a National Threat to Jewish Organizations

<table>
<thead>
<tr>
<th></th>
<th>Recommended Escalation Protocol:</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>2.1  Hold a brief meeting of the crisis management team and security committee.</td>
</tr>
<tr>
<td></td>
<td>2.2  Assign an individual to monitor national threats to determine if they could impact your JCC.</td>
</tr>
<tr>
<td></td>
<td>2.3  Establish communications with local, state and federal law enforcement to gather available information.</td>
</tr>
<tr>
<td></td>
<td>2.4  Assigned individuals should provide daily updates to the crisis management team.</td>
</tr>
<tr>
<td></td>
<td>2.5  Crisis management team should evaluate potential threat level to your organization and allocate resources.</td>
</tr>
<tr>
<td></td>
<td>2.6  Review and update current security strategies and crisis management planning.</td>
</tr>
<tr>
<td></td>
<td>2.7  Test electronic security and physical systems and controls.</td>
</tr>
<tr>
<td></td>
<td>2.8  Security systems and controls should be functioning correctly, and policies and procedures should be up to date and observed.</td>
</tr>
</tbody>
</table>
### 3. In the Event of a Statewide Threat to Jewish Organizations

<table>
<thead>
<tr>
<th>#</th>
<th>Recommended Escalation Protocol:</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Hold a meeting of the crisis management team and security committee that includes a briefing by the director or a senior member of the crisis management team.</td>
</tr>
<tr>
<td>3.2</td>
<td>Assign an individual to coordinate preparedness and liaise with law enforcement.</td>
</tr>
<tr>
<td>3.3</td>
<td>Establish communications with local, state and federal law enforcement to gather available information.</td>
</tr>
<tr>
<td>3.4</td>
<td>Establish communications with local Jewish organizations to gather information and share security concerns.</td>
</tr>
<tr>
<td>3.5</td>
<td>Assigned individuals should provide daily updates to the crisis management team.</td>
</tr>
<tr>
<td>3.6</td>
<td>The crisis management team should evaluate the potential threat level to your organization and allocate resources.</td>
</tr>
<tr>
<td>3.7</td>
<td>Review and update your current security strategies and crisis management planning.</td>
</tr>
<tr>
<td>3.8</td>
<td>Security systems and controls should be functioning correctly, and policies and procedures should be up to date and strictly observed.</td>
</tr>
<tr>
<td>3.9</td>
<td>Test all of your electronic and physical security systems and controls.</td>
</tr>
<tr>
<td>3.10</td>
<td>Repair or update all electronic and physical security systems that require attention.</td>
</tr>
<tr>
<td>3.11</td>
<td>If appropriate, escalate any repairs and/or installation of new security equipment.</td>
</tr>
<tr>
<td>3.12</td>
<td>Establish relationships with vendors that may be required to provide additional security services to your facility.</td>
</tr>
<tr>
<td>3.13</td>
<td>Provide, update or reinforce security training for staff with security responsibilities.</td>
</tr>
</tbody>
</table>

### 4. In the Event of a Threat to Similar Types of Organizations (Including Non-Jewish Within Your Geographic Area)

<table>
<thead>
<tr>
<th>#</th>
<th>Recommended Escalation Protocol:</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Hold a meeting of the crisis management team and security committee that includes a briefing by the director or a senior member of the crisis management team.</td>
</tr>
<tr>
<td>4.2</td>
<td>Assign an individual to coordinate your preparedness and act as a law enforcement liaison to gather information and provide daily updates to the crisis management team.</td>
</tr>
<tr>
<td>4.3</td>
<td>Establish communications with local, state and federal law enforcement to gather available information.</td>
</tr>
<tr>
<td>4.5</td>
<td>Establish communications with local Jewish organizations to gather information and share security concerns.</td>
</tr>
<tr>
<td>4.6</td>
<td>If other religious organizations are the current target of this threat, make an effort to meet with, gather information from and share security concerns with these organizations.</td>
</tr>
<tr>
<td>4.7</td>
<td>The crisis management team should assess the severity level of the threat to your JCC and take appropriate actions.</td>
</tr>
</tbody>
</table>
### 5. In the Event of Threats to Local Jewish Organizations

#### Recommended Escalation Protocol:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Hold a meeting of the crisis management team and security committee that includes a briefing by the director or a senior member of the crisis management team.</td>
</tr>
<tr>
<td>5.2</td>
<td>Assign an individual to coordinate your preparedness and act as law enforcement liaison to gather information and provide daily updates to the crisis management team.</td>
</tr>
<tr>
<td>5.3</td>
<td>Establish communications with local, state and federal law enforcement to gather all available information.</td>
</tr>
<tr>
<td>5.4</td>
<td>Establish communications with local Jewish organizations to gather information and share security concerns.</td>
</tr>
<tr>
<td>5.5</td>
<td>The crisis management team should assess the severity level of the threat to your JCC and take appropriate actions.</td>
</tr>
</tbody>
</table>
### 6. In the Event of Threats to Your JCC

<table>
<thead>
<tr>
<th>✓</th>
<th>In the Event Threat Has a Potential to Impact Your JCC, Additional Steps Should be Taken:</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.6</td>
<td>Review and update current security strategies and your crisis management plan.</td>
</tr>
<tr>
<td>5.7</td>
<td>Review your crisis management meeting and assembly areas, supplies and equipment to ensure that all are operational. Acquire any additional anticipated equipment and supplies.</td>
</tr>
<tr>
<td>5.8</td>
<td>Test all of your electronic and physical security systems and controls.</td>
</tr>
<tr>
<td>5.9</td>
<td>Update and repair electronic and physical security systems that require attention.</td>
</tr>
<tr>
<td>5.10</td>
<td>If appropriate, escalate any repairs and/or installation of new security equipment.</td>
</tr>
<tr>
<td>5.11</td>
<td>Ensure that security staff is familiar with all aspects of your electronic security systems, including running access control reports and reviewing video recording.</td>
</tr>
<tr>
<td>5.12</td>
<td>Brief security, reception, facility staff and anyone else with security-related duties on the current threat and their responsibilities.</td>
</tr>
<tr>
<td>5.13</td>
<td>You should be able to quickly and effectively lock down your facility.</td>
</tr>
<tr>
<td>5.14</td>
<td>Test all lockdown components and procedures and make any required modifications.</td>
</tr>
<tr>
<td>5.15</td>
<td>Ensure that video history is being reviewed on a daily basis.</td>
</tr>
<tr>
<td>5.16</td>
<td>Increase daily security inspections.</td>
</tr>
<tr>
<td>5.17</td>
<td>Meet and establish working relationships with any vendors that may be required to provide additional security services.</td>
</tr>
<tr>
<td>5.18</td>
<td>Request that local law enforcement conduct a security assessment of your facility.</td>
</tr>
<tr>
<td>5.19</td>
<td>Hire an independent security consultant to evaluate your operational procedures, systems and operational readiness with respect to the current threat.</td>
</tr>
</tbody>
</table>

### 6. In the Event of Threats to Your JCC

<table>
<thead>
<tr>
<th>✓</th>
<th>Recommended Escalation Protocol:</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Activate your crisis management team. Have the director or a senior member of the crisis management team brief your security committee. Conduct an initial assessment and implement enhanced security controls until a complete assessment of the situation can be conducted.</td>
</tr>
<tr>
<td>6.2</td>
<td>At a minimum, hold daily meetings with your crisis management team.</td>
</tr>
<tr>
<td>6.3</td>
<td>Assign an individual from your crisis management team to coordinate preparedness, liaise with law enforcement, gather information and update the crisis management team.</td>
</tr>
<tr>
<td>6.4</td>
<td>Communicate daily with local, state and federal law enforcement to gather available information.</td>
</tr>
<tr>
<td>6.5</td>
<td>Request an on-site law enforcement meeting and site review.</td>
</tr>
<tr>
<td>6.6</td>
<td>Communicate with local Jewish organizations to gather information and share security concerns.</td>
</tr>
<tr>
<td>6.7</td>
<td>Your crisis management team should assess the threat severity, develop a security strategy and allocate necessary resources.</td>
</tr>
<tr>
<td>6.8</td>
<td>Request to have police guards assigned to your facility.</td>
</tr>
<tr>
<td>6.9</td>
<td>Review your current security strategies and crisis management plan and update them to address current threats.</td>
</tr>
</tbody>
</table>
6.10 Hire an independent security consultant to evaluate your operational procedures, systems and operational readiness to meet the current threat.

6.11 Review your crisis management meeting and assembly areas, supplies and equipment to ensure all are operational. Acquire and test any additional equipment and supplies needed.

6.12 Conduct necessary drills and training to ensure a quick and appropriate response.

6.13 Test all of your electronic and physical security systems and controls.

6.14 Update and repair any electronic and physical security systems that require attention.

6.15 If appropriate, escalate any repairs and installation of new security equipment.

6.16 Ensure that security, reception and facilities staff are aware of the threat and their responsibilities.

6.17 Ensure that security staff is familiar with all aspects of your electronic security systems, including running access control reports, locking and unlocking doors and reviewing video recordings.

6.18 Ensure that your camera system is continuously monitored during operating hours.

6.19 Increase the reviewing of recorded camera activity (a minimum of twice a day).

6.20 Ensure that you are able to quickly and effectively lock down your facility.

6.21 Increase security inspections.

6.22 Conduct tabletop exercises concerning this threat.

6.23 Conduct additional security awareness training.

6.24 Instruct staff and membership to report any suspicious or unusual activity.

6.25 Evaluate your current security staffing and increase staffing if required.

6.26 Increase or implement exterior uniformed security patrols.

6.27 Initiate a counter-surveillance program to monitor the exterior of your facility.

6.28 Meet with security vendors, finalize requirements and sign agreements if required.

6.29 Evaluate the need for hiring off-duty police and/or security guards.

6.30 Restrict entrance and exit access to only secure and manned entrances.

6.31 Test that staff can quickly and effectively lock down the facility doors.

6.32 Implement vehicle and pedestrian checkpoints at the main entrance to the facility.

6.33 Consider keeping the main entrance door locked until each arriving person is identified as staff, member or visitor.

6.34 Consider postponing special events or adding security.

6.35 Consider closing the facility during peak threat times.

6.36 Consider modifying operating hours.

6.37 Limit and/or postpone exterior activities that could be at risk to this exposure.

Questions and Calls to Action

1. Depending on the nature of the threat, would you consider bringing together subgroups of the entire crisis management team to address the threat?

2. What crisis communications have been set up for each type of threat?

3. How robust is your emergency notification system?
SECTION G

GUARD FORCE MANAGEMENT CONCEPTS AND GUIDELINES
The vast majority of JCCs and camps contract with outside companies to provide guard service. This section is written with those JCCs and camps in mind. However, if your JCC is among the few that self-manage security, you should still review this section for applicable and relevant guidance.

The first step toward utilizing security guards efficiently is developing a scope of work for the bid process. Documenting your requirements will assist you in finding the right company with the right staff.

A successful program requires clear communications, defined areas of responsibility and staff awareness of employer expectations. Training is the cornerstone of a successful security guard program. Security guards must understand your environment, be in sync with your organization’s culture and be customer-service-oriented. A post order is a document that details what is expected of your security guards. For each post at which a security guard stands, there should be detailed post orders, which must be provided by your guard company and reviewed and approved by your organization.

Security Guard Failures

The majority of security guard failures are due to poorly defined post orders and/or a lack of training. Most of the remaining problems stem from guard companies’ poor hiring practices and lack of on-site management. Choosing the right security guard company and negotiating your contract properly is the first, and possibly the most critical, step. In addition to responding to an emergency, your security guard could be the first person to verbally or nonverbally greet a prospective member, donor, board member or senior member of the community. First impressions are important. Even though security guards are outsourced, they require constant management by site executives.

Post Orders: General

Post orders are the rulebook or written instructions that security guards follow while on duty.

They outline your policies and standard operating procedures, as well as your guards’ areas of responsibility and duties for each shift and/or each post.

Post orders cannot cover every possible event. They must cover what normally happens daily, weekly, monthly and on special occasions. They must also include guidelines for dealing with the unexpected. Understanding and following post orders will help a security guard make the right decision even under the most stressful circumstances.

Security guard companies will have a standard template for post orders. However, each individual organization must review the template post orders, provide input on their own policies and procedures and ensure that post orders cover all expectations for the security guards.

It is important to note that while you should provide guidance about the policies, procedures and expectations included the post orders for your organization, the post orders themselves are created and owned by the guard company. You should not assume the responsibility and potential liability for creating post orders.

Remember that guards are new to your organization. Even if they have worked in other facilities, the culture in those places might have been drastically different from yours, and techniques used in previous places of employment could be unacceptable to you and your membership. Often, when security guards are asked about a mistake in judgment, they will often reply that no one ever provided guidance on the situation in question. The guard is often left to do what he or she thinks is best to resolve a problem. This is why post orders should be finalized before the guards’ first day on-site.

Post Orders: General Rules and Expectations

Generally, post orders should include the following: guards should arrive on time; guards must not leave a post until they have been relieved; guards must be alert at all times; no use of personal phones or Internet while on duty; no eating while on duty, etc.

Contact Information

Contact information should include phone numbers of employees who are the guards’ points of contact, local emergency phone numbers, etc.

Reports

Security guards should create and submit daily reports and incident reports. Daily reports should detail everything that happened during the course of the day and incident reports should describe anything out of the ordinary or any emergency that occurred (as well as who was notified of the incident).

Policies and Procedures

Who is authorized to enter the building? What is the process for signing in visitors? What is the process for vendors or deliveries arriving at the facility?

Are there special access areas in the facility?

Who is authorized to access those areas?

What is the guard’s role during the arrival and dismissal of children? How should the security guard work with
other staff members to ensure the safe entry and exit of children from the facility?

**Recommendation**
Reviewing the entire security manual will assist you in developing an effective guard force management program.

**Post Orders:**
**Security Guard Company Contract**
As with any other business practice or outsourcing endeavor, focusing on the details of the contract with your guard company is critical. Key issues include security guard qualifications, training (continual on-site and off-site training), salary and benefits, on-site supervision and developing detailed post orders. Guard companies can be reluctant to develop detailed post orders, even if you stress this in every area of negotiations and document it in the final agreement. Do not be surprised if you receive very generic post orders. You and your staff may have to work very closely with the security guard company to ensure that their post orders are tailored to your facility. The more detailed the initial scope of work you deliver to the guard company, the easier the final post orders will be to develop. The final post orders should be reviewed and approved by both the security guard company and your organization, but published and owned by the security guard company. For liability reasons, the final version of post orders should always be the product of the guard company. Keep in mind, these are living documents that must be reviewed on a regular basis and updated when your environment or threat conditions change.

Post orders should be finalized before the guards’ first day on-site so that the guards have a chance to review and train with the post orders before they start at your location.

There are many reasons to have detailed, tailored post orders. Security guards are more confident in their duties when their scope of work is clearly defined. Should an assigned security guard be absent for a period of time, or should he or she resign, detailed post orders will smooth the transition to the replacement security guard. When things go wrong, post orders will help you determine who is at fault and what action should be taken. Post orders truly help security guards do a more professional job every day, build their self-respect and boost confidence in those they are assigned to protect. Good post orders will maximize your security guards’ value to your organization.

**Possible Security Guard Assignments**
Below is a list of some of the assignments, tasks and locations in which a security guard could add value. It does not address every possibility, and some may not be applicable to your location. Please note that if security guards are assigned multiple clerical tasks, they will not be able to efficiently perform their primary functions.

- Main gate
- Main door
- Reception
- Rear entrance
- Loading dock area or rear kitchen door
- Command center (monitoring cameras, alarms, access system, intercoms, etc.)
- Near campers and/or children in exterior recreational areas
- Respond to a medical emergency
- Respond to alarm activation
- Respond to bomb threat
- Perform interior roving patrols
- Perform exterior roving patrols
- Conduct daily internal and external inspections
- Locking and unlocking building areas
- Write reports
- Tend to childcare arrival and dismissal
- Tend to elevator entrapment
- Monitor external events (catering, auditorium events, lectures, parties, etc.)
- Interact with first responders
- Assist in building evacuation and or shelter-in-place events

**General Standard of Conduct**
A new security guard may not be familiar with your organization, culture and business environment.

**To ensure that security guards provide added value, they should behave in accordance with the following guidelines:**

1. Security guards must report for duty on time, in uniform and ready to start work.
2. A security guard should not leave his or her post until properly relieved by another security guard or authorized representative.
3. Security guards should know who in management to notify and notify management of any problems that occur. They should notify and/or ask for the assistance of their supervisor or JCC management whenever unusual incidents occur.
4. No personal use of JCC computers or the Internet while on post.
5. Security guards must not use client’s telephone for non-business calls. Personal cell phone use must be limited to breaks (except for some pre-approved personal emergency conditions).
6. No smoking, eating, chewing gum or reading of non-company related materials on post.
7. Sleeping, dozing or the appearance of sleeping on the job is cause for dismissal.
8. A security guard must wear a neat, complete, season-approved uniform on post at all times.

9. Security guards should not congregate with other security guards while performing duties (unless sharing work-related information), in order to avoid the perception (and reality) that security is not as alert or observant as it should be.

10. Security guards must be courteous and maintain a professional demeanor. Unnecessary conversation should be avoided. Conversations with members should be businesslike.

11. Security guards cannot be under the influence of alcohol or narcotics or smell of alcohol or narcotics while on duty.

12. Security guards should not do security site scheduling and/or payroll; this takes time away from security functions and should be completed by guard company office personnel only.

**Basic Guidelines for Dealing With the Public**

Security guards are expected to carry out their duties with professional courtesy and skill at all times. As visible JCC representatives charged with the responsibility of providing a secure environment, security guards are held to the highest standards of conduct.

**When dealing with the public, security guards should behave in accordance with the following guidelines:**

1. When at or near the front desk, security guards must remain alert. They are often a visitor's first impression of the JCC. They should behave in a professional manner and show a sincere effort to assist everyone.

2. Guards should avoid personal remarks or being overly friendly with staff, visitors and members. Use of offensive, racist or rude language and/or obscene gestures is prohibited. Guards are not to threaten or intimidate anyone in an attempt to demonstrate authority.

3. Security guards must be respectful, patient, diplomatic and polite at all times, even if the person they are dealing with is rude or disrespectful. Being firm in dealing with difficult people does not mean being discourteous. Guards must remain cognizant of the fact that their uniform makes them stand out; it is important they stand up straight, avoid leaning against walls, do not discuss personal matters while on duty in public areas and present an alert and competent image.

**Working With First Responders**

On occasion, the police or other governmental enforcement agencies will request to enter the facility in connection with official business. The JCC should cooperate with guards performing official duties. Security guards are responsible for facilitating this cooperation in a manner that minimizes disruption of your business activities.

**When interfacing with first responders, security guards should behave in accordance with the following guidelines:**

- Security guards must notify the JCC management team upon arrival of police guards or law enforcement agents at the facility.

- The security guard should ask law enforcement about the nature and purpose of their entry. Law enforcement agents should be asked to display proper identification, which must include an official law enforcement credential with photo identification.

- When the police are responding to an emergency situation, they must be allowed to proceed directly to the problem area. In an emergency situation, the first responders will be in charge upon their arrival at the scene of the emergency.

- In non-emergency situations, the guards should be directed to the JCC CEO/executive director.

- Assistance and cooperation must be extended to the police guards/law enforcement/first responder agents at all times.

- An incident report must be prepared regarding any incident involving police guards or law enforcement agents. The identities of the law enforcement guards involved and any pertinent information (complaint, voucher numbers, etc.) should be included.

- The JCC CEO/executive director or his/her designee will maintain a working relationship with the local police precinct and specialized enforcement units and will exchange information regarding problems occurring in and around the facilities.

**Incident Reports**

All incident reports must be written in a clear and concise manner. They should include an accurate and legible statement of the facts, as such reports are often used in legal and insurance matters. If called to testify in a legal proceeding, the written report is the basis of your testimony. Additionally, these reports often advise others of situations that require immediate additional action, such as the filing of legal charges after a suspect's arrest or the correcting of dangerous fire and safety hazards when they are discovered. Ensure that each report is correct in all details before signing.

1. When writing the report, remember to state clearly if you witnessed something and whether it was witnessed by others. If witnessed by others, record their statements word for word.
and include their names and associations to your JCC (staff, guest, member, contractor, trespasser, general public, etc.). If possible, take photographs of the area involved. Remember to include the following in your report:

- When did it happen (day of the week, date and time)?
- Where did it happen (exactly)?
- Who was involved?
- What happened?
- How did it happen?
- Why did it happen? What caused it?

2. Do not include your opinions—just the facts as they are stated and your observations.

3. Determine if the area is covered by the camera system. If so, secure (make a copy of) the recording, acknowledge its existence and provide a synopsis in the report.

4. The report should be written as though you were talking to someone about the incident. Think about why you are writing the report and who will be reading it. You may summarize an individual’s statements. However, if you would like to quote an important statement, you quote it exactly, using quotation marks.

5. Incident reports and the information contained therein are confidential; they may not be divulged to anyone outside of the approved individuals.

6. All incidents must be reported to the CEO/executive director or his/her designee as soon as possible. If the incident itself is still a risk to others, it must be immediately reported to the CEO/executive director, head of facilities and/or any other person designated to receive this information.

Security Inspections

While performing building and/or external security tours, security guards should utilize the JCC’s site inspection protocols (Section H). Be alert for and report security incidents, safety hazards, unauthorized persons and suspicious objects.

Where applicable, security guards must carry a radio at all times while on patrol. Portable radios should be checked to ensure that they are in proper working order at the start of each shift. Identified issues that relate to hazardous conditions and suspicious or unusual incidents must be immediately escalated to the JCC’s executive team.

Politely but firmly ask suspicious or unfamiliar persons what their business is in the building or on the premises, and if you can assist them in finding the area or person they are seeking.

When engaging a suspicious person in isolated areas of the facility, notify reception, facility management and/or site management of your location by radio. Radio for assistance if the individual refuses to cooperate, identify himself or provide a reason for being there.

Ensure that guards have all the proper equipment necessary to fulfill their assigned tour duties. They need to know how to use all equipment, including CCTV and access control, communications and alarm systems.

Security guards are expected to be familiar with:

- Every part of the facility, including interior and exterior recreational areas, departments, tenant spaces, etc.
- The locations of light switches, electrical panels and power switches
- The locations of fire and emergency exits, as well as private and public fire alarm boxes and firefighting equipment, including hydrants, hose reels and fire extinguishers
- The locations of vital mechanical equipment
- The locations of any hazardous material storage
- The locations of first-aid kits

Security guards are expected to understand the operation of:

- The general building systems
- The building fire alarm system, fire sprinkler system and fire extinguishers
- The building key management system
- The visitor management system
- The public address systems
- Two-way radios and service

Security guards are expected to know the protocol and procedures for:

- How to process mail and special deliveries (UPS, FedEx, DHL, Staples, food deliveries, facility supplies, etc.)
- Daily, weekly and monthly special events and activities
- All JCC security emergency protocols and guidelines
- All JCC security, safety and emergency management policies and procedures
- Executing an immediate lockdown
- Sheltering in place
All security guards are expected to know (or to have readily available) the telephone numbers of:

- Police, fire and rescue departments
- Site supervisors and facility management
- Members of senior management teams and/or their designees

Management’s Responsibility

At a minimum, management must review and update security guard post orders annually and/or when security conditions change.

**Management (or management designee) should also:**

1. Monitor security guards’ activity to ensure that they are complying with standards and guidelines. Inspect security guards’ operational proficiency, customer service skills, attention to detail, written reports, aptitude concerning inspections, uniform condition and use of personal communication devices.
2. Supply daily security updates (daily activity, upcoming events, previously reported security issues, known security problems, etc.) to security guards.
3. Review daily reports and make necessary responses to conditions reported.
4. Provide positive feedback to the security guard company when security guards go above and beyond.
5. Provide guidance when guards are deficient in their duties.

Conclusion

- Security guards can quickly become part of your organization’s image; when appropriate, you can provide direct feedback to security guards.
- A lot is expected of security guards, and often their compensation doesn’t match their contributions. Ideally, you should make them feel like they are part of the team they help protect. When negotiating with the security guard company, identify the security guards’ salary from the company markup. Markup can vary. Make sure the security guards are receiving a fair salary.
- Ensure that the guard company conducts weekly on-site security management and inspections. At minimum, they should conduct one inspection per shift (a.m./p.m.) during weekdays and one on weekends. You can negotiate for more on-site supervision and management.
- If you are located in a region that requires security guards to join a local union, be sure to be well-informed about all union requests and regulations.
- Request guards with security experience.
- If possible, request guards with experience in environments similar to that of your facility.
- Do not accept guards who were removed from other assignments for disciplinary reasons.
- Ensure that all guards are trained on your security systems (video, access control, etc.).
- Compare levels of insurance carried by guard companies you are considering.
- Try to negotiate terms for special events that would otherwise require overtime.
- Stipulate the level of education required.
- Require that guards be CPR, AED and fire extinguisher certified.
- Require the guard company to provide a replacement for an absent guard within one hour of his/her scheduled shift. The guard company should be held responsible for any overtime incurred due to an absent or late guard. Include a penalty if this requirement is not met.
- Make sure that you can immediately request that a guard be removed from your facility for inappropriate behavior without a penalty of any type.
- Remember that during negotiations, everything is on the table.
- Review your monthly invoice closely.

Questions and Calls to Action

1. Do post orders for guards accurately reflect the security needs of the JCC? When was the last time they were reviewed?
2. Does the guard company proactively review post orders with the JCC?
3. How often do security inspections occur?
4. Have incident reports been reviewed by the JCC’s insurance companies? By legal counsel?
5. What type of training takes place to acculturate guards to working with JCC populations?
SECTION H

INTEGRATING SITE INSPECTIONS INTO A SECURITY PROGRAM

WHY REGULAR INSPECTIONS ARE IMPORTANT
SECTION H.
SITE INSPECTIONS

INTEGRATING SITE INSPECTIONS INTO A SECURITY PROGRAM
WHY REGULAR INSPECTIONS ARE IMPORTANT

Standardized security site inspections are part of an effective security program. Inspections uncover substantial physical and electronic security equipment malfunctions, ineffective design concepts and inefficient system control settings that can otherwise go unnoticed for long periods of time. In addition, inspections can identify suspicious and/or hazardous objects, conditions and people; staff or member misconduct and the tampering with or neutralizing of security sensors and components.

Regular inspections of a facility can help assure that users and their families do not happen upon anything inappropriate or hazardous.

An active inspection program serves as a deterrent, demonstrating to ill-intentioned persons that security is taken seriously and constantly monitored.

Who Should Conduct Inspections?

Inspections should be conducted by security or facility personnel trained in your security staff awareness program, security policies and inspection procedures. Such personnel should be familiar with the workings of the facility and your property. Something clearly suspicious at one location may not be considered suspicious at another. While conducting inspections, your inspector should carry a cell phone or radio, an inspection checklist, additional writing material, a camera and a flashlight (depending on time of day and inspection areas).

Security Inspection Protocols

Create a security checklist to document and manage inspections. The person conducting the inspection must record the time of day, areas inspected, conditions found and actions taken, and take pictures of unfamiliar, suspicious or questionable conditions and anything that seems out of place. The report should assign each condition a status of high, medium or low to indicate order of priority. This person conducting the inspection should also sign the report clearly and legibly.

In high-priority situations, notations should include whether or not permanent or temporary solutions were implemented, as well as any recommended follow-ups, courses of action and/or corrections. In high-priority situations, appropriate management personnel should be immediately notified so senior management can enact emergency or crisis management plans when warranted.

If a severe hazard or condition is identified, the individual conducting the inspection should be able and authorized to take immediate action.

At a minimum, inspections should be scheduled daily. Inspection areas can be assigned to different times of day or shifts. Key areas should be inspected during each shift. Daily reports should be submitted to management upon completion of inspection. Management should review and prioritize any conditions requiring attention. All daily inspections should be reviewed weekly and analysis should be conducted monthly to assure that action has been taken on all open issues. Copies of daily reviews should be filed in a secure location and maintained for a minimum period of 18 months. Partial inspections should also be considered at strategic times, such as:

- Before child drop-off and child dismissal
- Prior to a high-occupancy, controversial or special event
- After a known incident or threat
- Following a security equipment upgrade, repair or modification
- Following construction in general areas of equipment or sensors

No general list can include all areas or aspects of inspection. A checklist should be compiled with knowledge of the facility, threat conditions, property, and functionality and security issues. No checklist can include every possible scenario. When utilizing a security checklist during an inspection, keep an open mind to ensure that all relevant conditions and observations—even those not specified on the checklist—are recorded.

What to Look for During an Inspection

What are some of the things that should draw the attention of inspection staff? Anything out of place, missing, modified, new, inoperable, unlocked, suspicious, inappropriate, potentially dangerous or dangerous should attract attention. This could include one or more suspicious persons, their actions, their lack of action or the object of their focus (security equipment or procedures). It could also include something left behind inadvertently or intentionally (in order to gauge response or response time).

Are doors and windows that should be closed and locked open? Are doors propped open? Are locks operating correctly? Are door-closers working efficiently? Are alarm sensors functioning? Are there signs of tampering?
Are dangerous chemicals locked away? Are restricted areas, computer systems and confidential information secured?

**Developing a Unique Security Checklist**

Each facility should develop an individual schedule and customized checklist dependent on its terrain, risk factors, local issues, concerns and security controls.

The points below will help you develop a unique checklist for your individual facilities. Add any additional points of interest to this list that concern your facility, including geographic location, threats, conditions or recommendations by local or federal law enforcement. Update your list as new circumstances arise and areas of concern change. Conduct a full list review semiannually at a minimum.

**Visual Inspection of Exterior Areas and Conditions**

- Any suspicious vehicles in the area (unattended gas or chemical delivery truck, car or van unattended for a prolonged period of time, vehicle smelling of chemicals, vehicle with visible questionable items, etc.)
- Any suspicious persons on or near the property (persons observing security operations, inspection of security equipment, children at play, children in pickup and drop-off areas, and/or opening and closing procedures, and/or displaying interest in chemical or fuel storage areas, open gates or doors, etc.)
- Unauthorized operational portable photographic or video recording (GoPro, hunting and trail cameras, etc.)
- Perimeter of buildings in which interior space is used as a safe haven or to shelter in place (should be free and clear of debris, suspicious or unknown items and include a close inspection of areas with plants, decorative shrubs or other items blocking the view of the inspector)
- Cameras and security sensors (appear functional, no tampering)
- Windows, doors, delivery areas and roll-up gates (secured)
- Playgrounds and playground equipment (free of hazardous or suspicious items or conditions)
- Preschool drop-off and pickup areas (free of hazardous or suspicious items or conditions)
- Sports fields, pools, play areas, hiking trails, etc. (free of hazardous or suspicious items or conditions or signs of unauthorized use)
- Parking lot areas (free of hazardous or suspicious items or persons)
- Perimeter fencing and gates (fencing is intact, limited space below fence to ground, locks functioning, nothing near fence to aid in climbing, gates close easily, limited space between gate and post, gates lock where applicable, etc.)
- Landscaping plants, shrubbery and planters (nothing hidden in the shrubs)
- Trash receptacles (can be used to conceal dangerous items)
- Bollard-type flower planters (can be used to conceal dangerous items)
- Graffiti or hate-related tagging
- “Private Property” and “No Trespassing” signs (should be visible from public side of property)
- Storage sheds, exterior bathrooms, changing rooms, field houses, etc. (areas secured, locks functioning; no signs of tampering, unauthorized access, safety issues, inappropriate items, etc.)
- Area above fabric or masonry awnings (can be used to conceal dangerous items)
- Adjacent wooded areas (signs of unauthorized use, debris, inappropriate items, etc.)
- Large trash receptacles picked up by truck (can be used to conceal dangerous items)
- Pool covers when installed (signs of tampering, safety issues, etc.)
- Waterways, ponds, water features, boat docks (security and safety issues)
- Exterior lighting (adequate illumination, bulb replacement needed, signs of tampering, dangerous wiring condition, etc.)
- Utility (gas, electric, etc.) building access points (signs of accidental damage, tampering, safety conditions, etc.)
- Visual inspection of neighboring high-rise buildings, residential or commercial space (to identify unusual levels of interest, unusual behavior, hate-related material, access points to property, etc.)

**Visual Inspection of Interior Areas and Conditions**

- Entrance and exit doors, emergency exits, loading dock areas, kitchen delivery doors, etc. (security controls functioning correctly; check door locks for signs of tampering)
- Doors to restricted areas (secured)
- Executive offices closed and locked (CEO/executive director office, accounting and HR departments, etc.)
- Sensitive document areas or cabinets (secured)
- Sensitive documents awaiting disposal (secured)
• Sensitive documents visible in open areas, such as stock or active employee and visitor IDs, checks, human resource documents, etc. (secured)
• Employee and member personal items in office areas, lockers, meeting rooms, etc. (secured)
• Emergency egress doors (locked and functioning correctly, close and relock automatically, alarm functioning, etc.)
• Safe haven or shelter-in-place locations (free and clear of suspicious or unknown items)
• Pathway to fire exit doors (free of debris)
• Roof access doors or hatch (secured and alarmed)
• Cameras and alarm sensors (functional and no tampering)
• Cleaning, maintenance and pool chemicals (appropriately stored and secured)
• Maintenance areas, theater, kitchen, auditorium (secured and clear of unknown or unauthorized items)
• Roll-down gates (functioning correctly and closed at appropriate times)
• Janitorial closets (locked)
• Hallways (clear of debris and unknown or unauthorized items)
• Interior lighting (functioning appropriately, requiring bulb replacement, etc.)
• Changing and locker rooms, auditorium, meeting rooms, pool area, gymnasium, etc. (no suspicious items left behind)
• Unauthorized operational portable photographic or video recording (GoPro, hunting and trail cameras, etc.)
• All ground floor and accessible doors and windows (closed and locked; note visible items that could be used to prop open doors, such as wood wedges, rocks, bricks or books)
• Basements, attics, storage areas, facility areas, meeting rooms, classrooms and bathrooms (secured, free of hazardous or suspicious items)
• Hazardous conditions observed (electrical, water, broken glass, etc.)

• Security-related cables and connections (in place and secure)

**Video**
• Video cameras (tested for functionality, pointing at the correct area and scene, limiting the amount of useless area, i.e. ceilings, floors, sky, intense light sources)
• Video camera recording system (recording appropriately: frames per second, duration, motion detection, storage capacity, etc.)
• Camera IP addresses (secured from unauthorized external viewing)
• Monitors (functioning clearly, providing usable picture)
• Security cabinets (free of hazards and secured)
• On-site staff (knowledgeable regarding search and display of recorded video, printing, exporting video footage, etc.)

**Access Control**
• Access control equipment (locks, door releases, etc., functioning properly and free from tampering)
• Access control database and recorded video data (secured, password-protected, backup available, access prohibited for unauthorized persons)
• On-site staff (knowledgeable regarding search of access control history, printing usage logs, time zones, access levels, alarm conditions, etc.)

**Emergency Equipment**
• Automatic lockdown equipment (test functionality)
• Intercom systems (test functionality)
• Emergency notification system (test functionality)

---

**Questions and Calls to Action**

1. Are regular site inspections occurring? Is the CEO/executive director doing spot-reviews to ensure that they are?
2. Who is conducting site inspections? How well-trained are they to do so?
3. When was the last time the site inspection security checklist was updated?
4. Are funds included in the annual budget for regular repairs/upgrades of security systems?
SECTION I

GUIDELINES FOR DEVELOPING A SECURITY COMMITTEE
SECTION I. GUIDELINES FOR DEVELOPING A SECURITY COMMITTEE

A security committee can be helpful in many ways. It will allow you to gather information and opinions, discuss potential strategies and draw on your committee members' professional expertise.

Different points of view will help form effective policies, procedures and strategies for dealing with security issues. People who are educated in security and risk management will enhance your overall security program. Having the right number of committee members is also important. Select enough committee members to provide expertise in many different aspects of security, but avoid selecting a group so large that it has difficulty coming to decisions and recommendations.

Usually a security committee does not make policy. Policies are made by executive stakeholders. Decisions that balance security and operational needs are never easy decisions. A security committee will help you explore risks, mitigate controls, manage the use of technology and determine the impact new controls and changes in policies will have on your general community.

Often, after you have established a security committee and acquainted its members with security concerns, controls and operational issues, a select group of security committee members can assist your crisis management team.

When forming your security committee, gather a diverse group of professionals. Committee members can be staff members, volunteers from your membership, or external professionals (college faculty, law enforcement, members of the local business community, etc.). In general, committee members should not be involved in selling services to your organization, and members should sign a confidentiality agreement before participating in the committee.

The expertise of committee members can vary greatly depending on location, availability of in-house specialists, security concerns and the official scope of the committee. For example, professionals in the following areas could have relevant training: law, medicine, mental health, HR, business management, marketing, security operations or integration, crisis and risk management and information technology.

Subcommittees can be appointed for more hands-on analysis, to conduct member surveys and inspections and to serve as volunteers during events or on short-term assignments.

Projects

Your security committee could study the need for, and impact of, some of the following:

• Closing secondary entrances and exits
• Restricting access to the main entrance
• Hiring uniformed security guards (unarmed and/or armed)
• Developing and implementing a formal crisis management team
• Creating a culture of security awareness among staff and membership
• Collaborating with other JCC security committees to benchmark security controls
• Studying local crime and/or anti-Semitic activity and its effect on membership
• Appointing personnel to plan and monitor special events
• Deciding whether to conduct active shooter drills
• Monitoring media sources and security bulletins for issues that could impact the organization
• Partnering with law enforcement by appointing someone to act as a security liaison for the JCC
• Reviewing, evaluating and implementing JCC Association’s security guidelines

First Steps

Deciding on the scope and purpose of the security committee should be your first step. Prepare a short document to ensure that there is a clear understanding of the committee’s purpose and committee members’ roles and responsibilities. The document should include an estimated time commitment for committee members.

Recruit committee members by open invitation and/or direct invitation to those you feel would have the most to offer. Usually, the more the purpose and scope of work of the committee is defined in the invitation, the more likely a candidate will accept the invitation.

New committee members will and should have varying opinions on the need and effectiveness of security controls in a community center. It is best to establish a balanced understanding of the issues before embarking on projects. Security decisions are often driven by emotion and an inaccurate understanding of threats and
controls. Committee composition should send a message that its decisions and recommendations have been carefully thought out.

The first meeting of your security committee should include an overview of security, risk management and effective security controls to mitigate unacceptable levels of risk. The introduction to this document provides a good basis for developing a presentation for your new committee members. Do not delegate this presentation to an external consultant or local law enforcement official unless you are confident that they can conduct the presentation in the stipulated manner. If you decide to engage an outside presenter, review and approve the entire presentation in advance. Any presentation should be tailored specifically to your objectives and your facility’s culture. Allow at least one hour for this portion of the meeting. If you feel more time is needed to ensure that committee members understand effective security concepts, schedule it during future meetings.

Include a discussion of potential risk to the organization (active shooter, anti-Semitic activity, terrorism, crime, liability issues, etc.), developing a proactive security culture (staff and membership) and establishing a balance between convenience and effective security strategies.

During the second half of your first meeting, present an overview of short- and long-term priority projects and a timeline for completing them. Assign a team leader for each project. Encourage committee members to be proactive and complete their assessments and/or projects in a timely fashion.

Keep minutes of all committee meetings and circulate them to committee members within three business days of each meeting. By the end of the first meeting, select one to three projects. For each of them, define goals and objectives and outline methods and set a timeline for completion. Team leaders should meet with their teams to develop strategies, and report back to the committee within seven to 10 business days. Before adjourning the meeting, establish a convenient date for the next meeting.

Once team leaders have submitted their outlines for each project, JCC senior leadership should review, evaluate, provide guidance on and approve a final approach and timeline.

### Pitfalls to Avoid

- **Lack of strong leadership and direction.** Because security is often a charged issue with many elements, the committee chair should be capable of directing a group of informed and passionate people and leading them to make recommendations.
- **Long and undefined meetings.** It is very possible to have meetings that react to the latest local, national or global security issue. Meetings should have well-defined agendas and relate to the matters at hand for the JCC.
- **Individuals overextending their authority.** It should be very clear who speaks for the committee on matters relating to JCC security. It would be good practice for committee members to not even signal their participation on the committee, letting its work take place in the background.
- **Members failing to respect the confidential nature of committee membership.** Expectations of confidentiality need to be clear from the very start. Specific security protocols should never be discussed out in the open.

### Questions and Calls to Action

1. After reading this section, is a security committee in the best interests of the JCC? If not, why not?
2. Consider the times security has been an issue for the JCC in the past year. What could a security committee do to help address these issues?
3. Who might be an excellent person to chair your security committee?
SECTION J

SECURITY GUIDELINES FOR
OFF-SITE MEETINGS AND EVENTS
At off-site events, there will probably be security exposures that merit consideration. However, you will have less direct control over the environment. There is always debate about whether more security is needed for off-site events than for events on your own property. This will depend on the level of security at your JCC, security conditions at the event location, current general threat levels and whether or not the meeting’s cause or agenda is controversial.

An off-site meeting that is small (20 or fewer participants), invitation-only, unannounced and held in a restaurant or office will probably not require much more attention. As meetings get larger, are announced to the general public, have on-site signage and/or focus on issues that cause conflict, your security exposures will increase. Off-site events with a higher volume of participants and with a greater exposure to the general public will have to balance a number of unknown circumstances. The information below should help you develop your security strategy and determine if you need additional security.

Pre-event planning is critical. Security must factor into your choice of event locations, hotels and transportation options. Organizers of large events will generally consider several venue locations. Many organizations do not conduct a thorough pre-event security evaluation, and venue locations often do not consider security as a major added value to their clients. Organizers often do not consider security until after an event location is chosen, which can result in the need to hire costly on-site security to correct unacceptable exposures (if detected). It is not unusual to find numerous security and safety concerns during a site review. Some major exposures could include ineffective access control; limited preparedness for emergencies; blocked fire egress doors and passageways; malfunctioning security equipment; bypassed security equipment; unalarmed restricted areas; unlocked fire exits; fire hazards; lack of fire extinguishers; unlocked exterior doors; uncontrolled access from maintenance, kitchen and delivery areas; no background checks on vendors and subcontractors, etc.

This guideline has been broken down into five sections to assist you in developing your approach to event security:

- General Concept
- Planning a Smaller Off-site Meeting
- Larger Event Security Strategy
- Large Event Security Checklist
- Event Opening Questionnaire (Two Weeks From Event)

### General Concept

The general security strategy for large or small events is similar in nature. Each will be effective in its own environment, but the scale and complexity will be different. In a small private meeting, it is only natural to restrict access to authorized people. Very little planning is required, and access can generally be controlled by the team managing the meeting.

As events start to get larger in scale, security concerns become more complex and require more planning and management. You could be dealing with venue and contract security personnel and procedures, multiple vendor relationships and a new physical location.

Always try to pick the best location that balances security and operational needs. Generally, a security director or manager should visit several locations with your event coordinator. Depending on the meeting type and threat level, balance security and safety concerns with the success of the overall event. You may find some venue locations more suitable for security purposes and less expensive to secure.

The level of security a venue provides is usually basic. A venue should not be responsible for developing your security plan. It is the host organization’s responsibility to conduct an analysis and to develop and implement necessary security controls. No one would expect the venue operator’s staff to select the theme, timing or choice of food at your event. Likewise, they should not develop your security plan.

In larger-scale environments that may utilize multiple interior and exterior locations (meeting rooms, locations occupied by children, multiple floors, lecture halls, auditoriums, gymnasiums, ball fields, etc.), the concept is the same.

### Five operational elements should govern security at these events:

- Create a perimeter.
- Monitor access points.
- Allow only authorized persons in.
- Continuously monitor for unauthorized persons.
- Be prepared to take quick and appropriate action.

Some events will require one or more additional limited-access areas (temporary office, speakers’ lounge, childcare, secure storage, etc.). Each of these will also require a physical and/or conceptual border. Steps must
be taken to ensure that only authorized persons access these areas.

Quickly identifying suspicious persons and activity is also critical in event security. With clearly defined parameters, appropriate credentials and the suitable number of security personnel (security guards, trained volunteers, etc.), unauthorized persons and/or intruders will be easier to spot.

Always issue event credentials. Participants should wear them at all times within the event perimeter. As participants leave the event, they should be instructed to take off and secure their credentials. Credentials should be unique and include the attendee’s name, access level (color coded), a recent photograph and, on the rear of the credential, emergency contact numbers. Depending on circumstances and threat levels, not all event security credentials should have the organization’s or associated organizations’ names or logos printed on the credential. Depending on the event type, additional information may be required.

Take credential photos on the day of the event. Such photos should be a minimum of 2 by 2 inches (although a larger photograph is recommended) and clearly represent the individual. At a minimum, a unique tamper-resistant hologram should be affixed to both sides of the credential. Generally, this is not a large expense, and it takes just a minute or two to take the photograph and print the ID of a preregistered guest. Each participant’s government-issued photo ID should be used to verify his or her identification before issuing credentials. If preferred, a participant can submit a recent photo (which must be reviewed on-site and clearly represent the individual) with their registration so credentials can be preprinted. Optional security information can be included on the rear of the credential (“security is everyone’s responsibility,” “immediately report suspicious activity to security,” security’s telephone number, assembly area instructions, etc.). Station credential-checkers at all interior and exterior perimeter access points.

Some open events may require a security review of participants before they are able to register. The level of background investigations will vary depending on the type of event and participants’ level of responsibility. Develop and strictly follow appropriate review criteria. If a review cannot be conducted at the event, unregistered persons should not be permitted to receive a credential.

Planning a Smaller Off-Site Meeting

When planning a smaller off-site meeting, safety and security should still be concerns. Factors to consider include whether the location is in a safe area and whether participants can travel to and from the location safely. Is the destination near any controversial locations? During the planning stages, someone should always review the location from a security and safety perspective. The day before an event, assess travel conditions (mass transit issues, road conditions, etc.) and local issues that could adversely impact your participants (such as protests). If the conditions become unfavorable, be prepared to postpone or relocate the event. These are very basic considerations that your meeting planner should consider in the early stages.

Larger Event Security Strategy

Larger events will require the same basic security standards. Provide a safe location for your event, allow only authorized individuals access, be alert and aware of suspicious activity and be prepared to respond to emergencies. Also understand that venues’ basic security is generally limited and focused on protecting the venue’s assets. Additional security is generally required. Your JCC security team (which can include volunteers and consultants) should develop your event security strategy, and your final security expectations must be very clearly defined within the venue agreement.

It is important to ensure there are no gray areas or gaps in security responsibilities and controls. A good way to do this is to have a security professional (in-house security director, security volunteer, security consultant, etc.) take responsibility for planning and managing security during the event. A qualified person would have extensive knowledge and experience in event security planning; the time to fully coordinate law enforcement, private security, volunteers and venue security; and an understanding of the limitations of each of these groups. Law enforcement could offer to take on responsibility for managing the event, but local law enforcement might not be officially and/or legally authorized to act in this capacity or trained in all the particular circumstances of event security.

Law enforcement has a critical role in providing a safe environment for events of this nature. Their monitoring of intelligence can prevent an incident. Their presence can act as a deterrent and, in the event of an emergency, their quick action can limit the impact of a hostile actor. However, in private-sector events, law enforcement generally does not coordinate all security operations. Police guards would rarely develop your security strategy, manage your security program, stand posts, check IDs, conduct counter-surveillance, etc. They do not address gaps in planning and responsibilities among venue security, security volunteers, executives, etc. Their experience, training and responsibility to the public do not meet all of your needs. Other issues that could have a negative impact on your event if you rely too heavily on law enforcement assistance may include:
• Other policing matters may arise simultaneously with your event, resulting in a reduction of the number of guards who can be assigned to assist you.
• Emergencies may arise during your event, necessitating the diversion of guards away from your site.
• JCCs may have no control or knowledge of where police will be located.
• There could be limited coordination, due to guards who are unfamiliar with your organization, location or event.

Recently, local police provided protection for an event at a hotel. They had not received any direction other than to go to the hotel on the designated day. Numerous areas of concern were identified during the event. The fact that nothing adverse happened during the event did not mean that there was effective security in place. Unfortunately, this was not an isolated incident.

Sometimes, it is difficult for individuals trained in different areas of security, policing or business management to understand the differences among various types of protective security strategies. Security strategies are not policing strategies. Event security is a specialty area of security. A professional with a background in dignitary protection, executive protection, policing or general security management is not necessarily qualified to conduct event security. Protecting a governor, diplomat or musician in a large crowd is very different from trying to protect the large crowd itself.

As part of the evaluation process, conduct a full review of the perimeter of all areas designated for use at the event. Check all entrance and exit doors to ensure that they are functioning and locked, including doors utilized by event staff. Make sure that electronic security systems are working correctly. Ensure that area cameras are in place, operational and being recorded and monitored.

An effective way to review and finalize security plans is to acquire site drawings of each of the venues to be used, adding all security plans to the drawings. Markings on these drawings should include:
  • Perimeter fencing
  • Accessways
  • Exterior grounds
  • Building perimeters
  • The perimeter of areas that are designated for JCC use within each building
  • Any security controls or technology (cameras, access controls, electronic security systems, communications equipment, defibrillators and controls that will assist during the event at each location)

Note where security components, equipment, staff and assets will be located. Police guards, off-duty police guards, venue security, outsourced security and/or volunteers should also be included. Include security responsibilities for each staffing post. Note your transportation security strategy. Once this process is complete, a quick review will provide a high-level overview of security planning and show any areas that need modification. You may choose to request the assistance of law enforcement in conducting this review as you finalize your strategy and discuss law enforcement’s contributions to your detailed security plans.
**Large Event Security Checklist**

Below is a detailed checklist that will help you develop your security plan.

All the points discussed will not be applicable to every event. Utilizing the list will assist you in developing your final security strategy. It must be stressed that no security checklist can include all relevant issues that can be encountered. Its purpose is to get you thinking in a logical manner about the many security matters that need to be addressed.

Your review of the completed checklist should include all of the issues that will need to be addressed during this event. It has been broken down into four modules, venue concerns, internal advanced planning, event credentials, emergency plans.

<table>
<thead>
<tr>
<th><strong>Venue Concerns</strong></th>
<th><strong>Notes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Are there contract terms that define responsibilities or limitations concerning security?</td>
<td></td>
</tr>
<tr>
<td>2. Does the venue have in-house security? Will they support the event?</td>
<td></td>
</tr>
<tr>
<td>3. Who will be your primary security point person throughout the planning stages and during the event?</td>
<td></td>
</tr>
<tr>
<td>4. Can this person supply cell phone numbers for all key security contact persons?</td>
<td></td>
</tr>
<tr>
<td>5. Can the venue supply you with a set of drawings to help develop your security strategy?</td>
<td></td>
</tr>
<tr>
<td>6. Are there sufficient in-house security personnel to secure the event?</td>
<td></td>
</tr>
<tr>
<td>7. Are they proprietary guards?</td>
<td></td>
</tr>
<tr>
<td>8. Does the facility use armed security guards?</td>
<td></td>
</tr>
<tr>
<td>9. Does the facility use off-duty police guards?</td>
<td></td>
</tr>
<tr>
<td>10. Is there a weapons policy for at the venue (JCC staff, volunteers, guests, etc.)?</td>
<td></td>
</tr>
<tr>
<td>11. Is there an identification process for armed outside security staff (JCC)?</td>
<td></td>
</tr>
<tr>
<td>12. Has the location received any recent threats against the location itself or against previous clients?</td>
<td></td>
</tr>
<tr>
<td>13. Does the venue have a preferred vendor list for contract security services (security guards, etc.)?</td>
<td></td>
</tr>
<tr>
<td>14. Have you requested permission for your security team to conduct a detailed security review of the facility?</td>
<td></td>
</tr>
<tr>
<td>15. Will the venue provide secure storage areas for your use?</td>
<td></td>
</tr>
<tr>
<td>16. Is there an access control, CCTV or intrusion detection system in place for the venue?</td>
<td></td>
</tr>
<tr>
<td>17. Is the access control and CCTV system monitored onsite?</td>
<td></td>
</tr>
<tr>
<td>18. Does the venue have staff available to respond to suspicious activities and/or alarm activations that will be functional during your event?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>19.</td>
<td>Will your security team have access to the venue’s command center and video and alarm monitoring?</td>
</tr>
<tr>
<td>20.</td>
<td>Can you have access to the venue’s radio frequency?</td>
</tr>
<tr>
<td>21.</td>
<td>Are all accessways to your event area covered by CCTV cameras and a door central alarm?</td>
</tr>
<tr>
<td>22.</td>
<td>If there is a need to monitor sensitive areas or equipment with the venue’s CCTV, will they accommodate the request, and will there be any additional cost?</td>
</tr>
<tr>
<td>23.</td>
<td>If need be, will you be able to quickly retrieve video images? What is the process for doing so?</td>
</tr>
<tr>
<td>24.</td>
<td>Are security doors/entrances alarmed (day and night systems) and in working order?</td>
</tr>
<tr>
<td>25.</td>
<td>In case of fire or evacuation, will emergency egress doors automatically unlock (fail-safe)?</td>
</tr>
<tr>
<td>26.</td>
<td>Will the venue provide proximity cards to your security personnel?</td>
</tr>
<tr>
<td>27.</td>
<td>Will event parking be provided? Is it secured?</td>
</tr>
<tr>
<td>28.</td>
<td>Have designated parking areas been determined? Is there enough capacity to accommodate all attendees?</td>
</tr>
<tr>
<td>29.</td>
<td>Will parking utilize valets and/or outside vendors?</td>
</tr>
<tr>
<td>30.</td>
<td>What process do you have in place for background checks of third-party persons or vendors involved in the event, and to what extent (employment history, criminal record, etc.)?</td>
</tr>
<tr>
<td>31.</td>
<td>Will any traffic patterns or vehicular movement near the event site potentially pose a risk to attendees?</td>
</tr>
<tr>
<td>32.</td>
<td>Is there any construction scheduled during your event?</td>
</tr>
</tbody>
</table>

**Internal Advance Planning**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>33.</td>
<td>Will the event be advertised to the public?</td>
</tr>
<tr>
<td>34.</td>
<td>Will the event have signage?</td>
</tr>
<tr>
<td>35.</td>
<td>Will the event be broadcast? If so, will it be live, live to tape or recorded?</td>
</tr>
<tr>
<td>36.</td>
<td>Will any part of the event be outdoors?</td>
</tr>
<tr>
<td>37.</td>
<td>Is there anything at the event site that could become dangerous due to weather?</td>
</tr>
<tr>
<td>38.</td>
<td>Is there a body of water near the event site that could pose a risk?</td>
</tr>
<tr>
<td>39.</td>
<td>Can you identify the security assignments/posts that require staffing (inner, middle and outer perimeter, all transport routes, parking)?</td>
</tr>
<tr>
<td>40.</td>
<td>Can you determine how many personnel will be needed at each assignment/post?</td>
</tr>
<tr>
<td>41.</td>
<td>Are there adequate post orders in place?</td>
</tr>
<tr>
<td>42.</td>
<td>Will customized post orders be required?</td>
</tr>
<tr>
<td>43.</td>
<td>Who will develop post orders?</td>
</tr>
<tr>
<td>44.</td>
<td>How many supervisors will be needed to oversee security personnel?</td>
</tr>
<tr>
<td></td>
<td>Question</td>
</tr>
<tr>
<td>---</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>45.</td>
<td>Will shifts be required for pre-event, event and post-event coverage?</td>
</tr>
<tr>
<td>46.</td>
<td>Who will do a site inspection each morning before the space is occupied?</td>
</tr>
<tr>
<td>47.</td>
<td>Will a relief security guard be required during the event and/or overnight?</td>
</tr>
<tr>
<td>48.</td>
<td>Is there a need for one or more security guard rovers?</td>
</tr>
<tr>
<td>49.</td>
<td>Can you supplement the venue’s security with your own security personnel or security volunteers?</td>
</tr>
<tr>
<td>50.</td>
<td>Will law enforcement be required for the event?</td>
</tr>
<tr>
<td>51.</td>
<td>Must local police be notified?</td>
</tr>
<tr>
<td>52.</td>
<td>Are K-9 bomb inspections needed?</td>
</tr>
<tr>
<td>53.</td>
<td>Are magnetometers and/or bag inspections necessary?</td>
</tr>
<tr>
<td>54.</td>
<td>Do you have a process in place to communicate regularly with key partners?</td>
</tr>
<tr>
<td>55.</td>
<td>Will public figures (heads of state, celebrities, corporate executives, VIPs/talent, religious figureheads, etc.) attend the event?</td>
</tr>
<tr>
<td>56.</td>
<td>Must you partner with additional security services for skills, equipment or technology support?</td>
</tr>
<tr>
<td>57.</td>
<td>Do you need to develop training in key specialized areas for security personnel or volunteers?</td>
</tr>
<tr>
<td>58.</td>
<td>Should you develop detailed instructions for volunteer security team members?</td>
</tr>
<tr>
<td>59.</td>
<td>Have you conducted a comprehensive training needs assessment to identify specialized knowledge and skills to implement the event security plan?</td>
</tr>
<tr>
<td>60.</td>
<td>Do you have sufficient training resources in-house or among outside vendors, volunteers or agencies?</td>
</tr>
<tr>
<td>61.</td>
<td>Have you developed the most effective and efficient training methods to reach required personnel prior to the event?</td>
</tr>
<tr>
<td>62.</td>
<td>Will there be a need to increase security for any part of the event (stage performances, VIPs, etc.)?</td>
</tr>
<tr>
<td>63.</td>
<td>Will you be able to clearly specify perimeters: inner, middle, outer, other? Do all those involved know the boundaries of those perimeters?</td>
</tr>
<tr>
<td>64.</td>
<td>Is there adequate and appropriate security for each perimeter?</td>
</tr>
<tr>
<td>65.</td>
<td>Is there enough technical equipment for effective and efficient screening?</td>
</tr>
<tr>
<td>66.</td>
<td>Have you chosen a location to issue credentials?</td>
</tr>
<tr>
<td>67.</td>
<td>Is there adequate staff for timely screening?</td>
</tr>
<tr>
<td>68.</td>
<td>Are staff trained and experienced in screening?</td>
</tr>
<tr>
<td>69.</td>
<td>Have appropriate screening protocols been developed and distributed? Have staff been trained in these protocols?</td>
</tr>
<tr>
<td>70.</td>
<td>Will visitors and participants be made aware of your screening protocols?</td>
</tr>
<tr>
<td>Question</td>
<td>Answer</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Are screening regulations clearly posted for guests?</td>
<td></td>
</tr>
<tr>
<td>Will re-entry be allowed?</td>
<td></td>
</tr>
<tr>
<td>Does the nature or theme of the event raise the threat level?</td>
<td></td>
</tr>
<tr>
<td>Will the presence of certain event attendees (VIPs) increase the overall threat level?</td>
<td></td>
</tr>
<tr>
<td>Will there be a designated area for press/media?</td>
<td></td>
</tr>
<tr>
<td>Do you have adequate intelligence support to conduct threat and risk assessments?</td>
<td></td>
</tr>
<tr>
<td>Should you employ intelligence resources in the field during the event?</td>
<td></td>
</tr>
<tr>
<td>Does the event, production or other entity have effective intelligence capability to monitor and report potential threats?</td>
<td></td>
</tr>
<tr>
<td>Is there a need for social media monitoring prior to the event?</td>
<td></td>
</tr>
<tr>
<td>Can you receive support from a local, state or federal agency with social media monitoring and intelligence capabilities?</td>
<td></td>
</tr>
<tr>
<td>Should a social media “geo-fence” be used?</td>
<td></td>
</tr>
<tr>
<td>Have you received useful and reliable intelligence regarding the potential for protest activity before or during the event?</td>
<td></td>
</tr>
<tr>
<td>Do the threat and risk levels for the event require involvement from law enforcement and other resources?</td>
<td></td>
</tr>
<tr>
<td>Do you have adequate communications technology and equipment?</td>
<td></td>
</tr>
<tr>
<td>Do you have adequate communications backup?</td>
<td></td>
</tr>
<tr>
<td>Is there a need for a prepopulated mass notification group for emergency messaging?</td>
<td></td>
</tr>
<tr>
<td>Can you integrate radio communication with the venue, vendors or agencies involved?</td>
<td></td>
</tr>
<tr>
<td>Will the food setup area be in a secured area?</td>
<td></td>
</tr>
<tr>
<td>If applicable, is there a plan to monitor the consumption of alcohol and to manage guests who overindulge?</td>
<td></td>
</tr>
<tr>
<td>Will there be live animals that could pose a potential risk?</td>
<td></td>
</tr>
<tr>
<td>Will there be fireworks, pyrotechnics, hazardous material or other fire-related dangers?</td>
<td></td>
</tr>
<tr>
<td>Will there be temporary structures, props or decorations that could pose a potential risk?</td>
<td></td>
</tr>
<tr>
<td>Will there be rides, inflatables or mechanical devices that need to be monitored?</td>
<td></td>
</tr>
<tr>
<td>Will there be a requirement for the protection of money or high-value assets?</td>
<td></td>
</tr>
<tr>
<td>Have protective measures against a cyber-attack been considered?</td>
<td></td>
</tr>
<tr>
<td>Event Credentials</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------</td>
</tr>
<tr>
<td>96. Will access to the event be private (credential or ticket required)?</td>
<td></td>
</tr>
<tr>
<td>97. Is there a plan and process to produce credentials for the event?</td>
<td></td>
</tr>
<tr>
<td>98. Will the credentialing process be handled in-house?</td>
<td></td>
</tr>
<tr>
<td>99. Will there be different access levels, and are they easy for security personnel to interpret?</td>
<td></td>
</tr>
<tr>
<td>100. Has adequate information been provided on credentials to verify the identity of guests and their level of access?</td>
<td></td>
</tr>
<tr>
<td>101. Do credentials include enough security features to prevent counterfeiting and assist in credential verification?</td>
<td></td>
</tr>
<tr>
<td>102. Who will be responsible for developing guidelines for credentialing (layout, information, photo, etc.)?</td>
<td></td>
</tr>
<tr>
<td>103. Will be responsible for acquiring the credentials?</td>
<td></td>
</tr>
<tr>
<td>104. Will both sides of the credential be printed and/or have a security hologram?</td>
<td></td>
</tr>
<tr>
<td>105. Are there specific requirements for who receives a credential?</td>
<td></td>
</tr>
<tr>
<td>106. Have criteria been determined to exclude people from receiving badges?</td>
<td></td>
</tr>
<tr>
<td>107. Who will be responsible for credentialing production?</td>
<td></td>
</tr>
<tr>
<td>108. Is there a designated area for credential pickup?</td>
<td></td>
</tr>
<tr>
<td>109. Will credential pickup be open prior to the event?</td>
<td></td>
</tr>
<tr>
<td>110. Will credential pickup be open during the event?</td>
<td></td>
</tr>
<tr>
<td>111. Will press/media have a designated credential?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Emergency Plans</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>112. Does the venue have adequate evacuation plans?</td>
<td></td>
</tr>
<tr>
<td>113. Do you have response plans for managing threats?</td>
<td></td>
</tr>
<tr>
<td>114. Are venue emergency plans up to date?</td>
<td></td>
</tr>
<tr>
<td>115. Is there a need for specialized medical vehicles and equipment?</td>
<td></td>
</tr>
<tr>
<td>116. Will EMS or an on-site medic be required?</td>
<td></td>
</tr>
<tr>
<td>117. What is the venue capacity?</td>
<td></td>
</tr>
<tr>
<td>118. Does it factor in configuration changes for the event?</td>
<td></td>
</tr>
<tr>
<td>119. Will the number of estimated attendees reach or surpass the venue capacity?</td>
<td></td>
</tr>
<tr>
<td>120. Is there a designated area for emergency response vehicles and personnel?</td>
<td></td>
</tr>
<tr>
<td>121. Are floorplans (showing AED locations, electrical, HVAC systems, etc.) available for event facilities?</td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td>Answer</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>122. Is there a primary hospital that would be used?</td>
<td></td>
</tr>
<tr>
<td>123. Where is the nearest trauma center?</td>
<td></td>
</tr>
<tr>
<td>124. Are there adequate plans for fire and EMS services’ response if needed?</td>
<td></td>
</tr>
<tr>
<td>125. Have key security and event organizers agreed on criteria for designating an evacuation?</td>
<td></td>
</tr>
<tr>
<td>126. Are there adequate protocols for handling bomb threats?</td>
<td></td>
</tr>
<tr>
<td>127. What is the standard protocol for bomb threats?</td>
<td></td>
</tr>
<tr>
<td>128. Does the venue immediately evacuate for bomb threats?</td>
<td></td>
</tr>
<tr>
<td>129. Is the evacuation plan up to date (e.g., does it take into account any facility redesign)?</td>
<td></td>
</tr>
<tr>
<td>130. Has the evacuation plan been approved by the fire department, fire marshal or other city or county inspections office?</td>
<td></td>
</tr>
<tr>
<td>131. Does the plan designate an overall emergency evacuation coordinator?</td>
<td></td>
</tr>
<tr>
<td>132. Does the plan show floorplans with marked evacuation routes?</td>
<td></td>
</tr>
<tr>
<td>133. Are exits clearly marked and designated for evacuation?</td>
<td></td>
</tr>
<tr>
<td>134. Does the plan include assistance for handicapped individuals?</td>
<td></td>
</tr>
<tr>
<td>135. Is there a designated assembly point for evacuations?</td>
<td></td>
</tr>
<tr>
<td>136. Does the venue have a procedure for an active shooter?</td>
<td></td>
</tr>
<tr>
<td>137. Are there defined safe haven areas?</td>
<td></td>
</tr>
<tr>
<td>138. Is there an active-shooter strategy to escape the facility?</td>
<td></td>
</tr>
<tr>
<td>139. What is the evacuation protocol for an active threat?</td>
<td></td>
</tr>
<tr>
<td>140. Have emergency traffic routes been planned?</td>
<td></td>
</tr>
<tr>
<td>141. Have specific evacuation security posts been identified to provide directions to the exiting crowd?</td>
<td></td>
</tr>
<tr>
<td>142. Does the facility post or broadcast evacuation messages to attendees prior to an event?</td>
<td></td>
</tr>
<tr>
<td>143. Does the facility conduct periodic emergency evacuation drills?</td>
<td></td>
</tr>
<tr>
<td>144. Is there a need for a public information and media relations plan?</td>
<td></td>
</tr>
<tr>
<td>145. Has a public information specialist or spokesperson been identified to coordinate communications?</td>
<td></td>
</tr>
<tr>
<td>146. What is the strategy for impromptu demonstrations?</td>
<td></td>
</tr>
<tr>
<td>147. Is local law enforcement aware of a potential demonstration?</td>
<td></td>
</tr>
<tr>
<td>148. Will law enforcement engage demonstrators prior to the event to discuss expectations and requirements?</td>
<td></td>
</tr>
<tr>
<td>149. Is law enforcement available to make arrests if necessary?</td>
<td></td>
</tr>
</tbody>
</table>
150. Has an event contact list been developed?

151. Is a complete list of VIPs, executives and performers available?

152. Is a contact list and details for each VIP’s handler available?

153. Will any of the VIPs, executives or performers have a security detail?

154. Is a complete list of VIP entourage or additional guests (including children) available?

155. Are there special needs or arrangements for VIPs?

156. Will VIPs, executives or performers be required to wear credentials?

### Event Opening Questionnaire

(Two Weeks From Event)

When you are two weeks from the start of your event, review the checklist below. It will help you determine if you are ready for the event. It is broken down into questions and answers to help you have confidence moving into the final days before your event starts.

<table>
<thead>
<tr>
<th></th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Do all applicable groups (staff, volunteers, law enforcement) know what to look for in identifying properly credentialed athletes, artists, coaches, staff, volunteers, guests and spectators? Is the process of developing on-the-spot spectator passes and replacement credentials well-known? It is incumbent upon the JCC to have practices and procedures in place to identify proper credentials and to determine what to do in the absence of or loss of credentials. Are there to be on-the-spot replacement passes?</td>
</tr>
<tr>
<td>2.</td>
<td>Are you following local, domestic and international security events that might impact your event? Have you checked with law enforcement concerning any new threats? Are you capable of making changes in your security plan if need be? Such security events can have an adverse impact on security requirements. Monitor these events from now through the end of your event. Be prepared to modify a security posture should the need arise to do so.</td>
</tr>
<tr>
<td>3.</td>
<td>Have you recently checked with your venue locations to ascertain if there have been any recent changes to security conditions, including other events to be held at the venue simultaneously? Have you checked with law enforcement to ensure their continued participation? Make sure that local and regional security conditions have not changed, and that there have been no security-related changes at the locations you will use. Check to see if there are any new public or private events planned in any of these areas. There could be conditions and events that would mandate a change in transportation routes, a change in the deployment of security staff and/or the availability of law enforcement assigned to your event. Monitor these conditions throughout your event.</td>
</tr>
<tr>
<td>4.</td>
<td>Have you determined whether your venues will have ongoing construction work that will impact attendee access and proceedings at your event or that will bring new workers into the environment during your event? Physical changes to event sites can sometimes occur. Road work or construction can change access points, and facility modifications or repairs can impact access and local security requirements. Last-minute additions of personnel on-site (contractors, subcontractors, construction workers, etc.) should warrant additional attention. These individuals may not be as well-vetted as regular on-site staff. The presence of delivery personnel and repair workers on-site and close to an event could be responsible for a spontaneous incident. This type of activity could necessitate alterations to your security strategy. Conduct a site review at each location one week before the event, as well as a second review the day before the start of the event.</td>
</tr>
<tr>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>---</td>
<td>-------------</td>
</tr>
<tr>
<td>5.</td>
<td>Have you recently checked with venue locations concerning the functionality of security equipment? Is everything in working order? Have there been any changes to their systems?</td>
</tr>
<tr>
<td>6.</td>
<td>Camera, access control and communications equipment at a site could have been recently upgraded or no longer be functional. In some cases, additional equipment that will assist in providing a secure environment might be available. Explore these possibilities at each site.</td>
</tr>
<tr>
<td>7.</td>
<td>Have you assigned security personnel to all high-risk areas? In an interior environment (basketball court, swimming pool, meeting room, dining facilities, etc.), all secondary entries/exits, fire egress doors, delivery access points and backstage doors should be controlled and monitored to ensure that unauthorized persons do not access the event.</td>
</tr>
<tr>
<td>8.</td>
<td>Have you considered monitoring all entrance and exits? Have you checked with the event management to determine controls and exposures?</td>
</tr>
<tr>
<td>9.</td>
<td>In the case that only a portion of the facility is being used for your event, pay special attention to common areas that provide access to the event (kitchen, delivery and staff entryways, etc.).</td>
</tr>
<tr>
<td>10.</td>
<td>If you are using a venue that features a public restaurant, are delivery areas to that restaurant monitored and staff vetted?</td>
</tr>
<tr>
<td>11.</td>
<td>If a public restaurant or similar type of venue is being used, access through delivery areas in the kitchen should be monitored. Remember that staff will not be well-vetted, and they should be monitored closely.</td>
</tr>
<tr>
<td>12.</td>
<td>Have you reviewed public space with law enforcement?</td>
</tr>
<tr>
<td>13.</td>
<td>In an exterior and public environment with soft borders or no borders, such as a sports field, pay extra attention to unauthorized spectators and suspicious persons and activity. Check with law enforcement what their plans are for such spaces.</td>
</tr>
<tr>
<td>14.</td>
<td>Have you discussed protection strategy in branded events with law enforcement or an event security specialist?</td>
</tr>
<tr>
<td>15.</td>
<td>If an event is advertised and/or publicly known, or if participants are branded, visible security should be present. Security should include the ability to detect suspicious activity early, take appropriate action and provide immediate direction to spectators and participants. Taking appropriate action could include direct interaction with suspicious persons or hostile actors. Those interacting with the threat should be trained security or law enforcement professionals.</td>
</tr>
<tr>
<td>16.</td>
<td>If you are using law enforcement guards, have you considered alternative plans if they are unavailable? Because there can be a lapse of on-duty law enforcement guards during shift changes, and because guards can be withdrawn to respond to other types of public emergencies during JCC events, staff should be prepared to manage all aspects of security.</td>
</tr>
<tr>
<td>17.</td>
<td>Have you reviewed all of your venue locations to determine if they have adequate security? Have you discussed this with law enforcement and/or venue security persons?</td>
</tr>
</tbody>
</table>
Conclusion

- Meet with logistical staff. Security staff should be an integral partner in planning the event.
- Conduct extensive pre-event planning to ensure security is part of the decision-making process when identifying a venue. Participate in all preliminary meetings, conduct a detailed security assessment of the chosen location(s), complete an event security checklist and meet with venue security personnel and law enforcement.
- Conduct site research. Know the sites, surrounding area and criminal trends.
- Conduct event security management two weeks from the event. Review and coordinate all aspects of security and emergency response.
- Just prior to the event, conduct a secondary security review of all aspects of the event to ensure that security arrangements are still within acceptable range.
- Conduct a full final review prior to the event opening. Be prepared to make changes if necessary. Conduct a full review (detailed inspection) every day prior to opening the event.
- Immediately after the event, ensure that breakdown of the event is without incident and that staff and assets are protected.
- Event recap: Go over lessons learned, meet with shareholders and prepare a final report.
SECTION K

SECURITY JOB DESCRIPTION:

CREATING A JOB DESCRIPTION FOR THE LEAD PROFESSIONAL OR CONSULTANT OVERSEEING SECURITY AT A JCC FACILITY
SECTION K.
SECURITY JOB DESCRIPTION:
CREATING A JOB DESCRIPTION FOR THE LEAD PROFESSIONAL OR CONSULTANT OVERSEEING SECURITY AT A JCC FACILITY

Job Description
To ensure that you hire the right person, start by developing a detailed job description, including areas of responsibilities and objectives. It will be necessary to have knowledge of existing and/or planned security programs in order to find the right person to run these programs.

Background
There are different requirements for applicants who will manage a security guard force as opposed to managing armed security professionals or developing an integrated security management program for a JCC. Many individuals transition into security management positions after prestigious careers in law enforcement. There is a vast difference between areas of responsibility and protocols in law enforcement and in private-sector security management positions. While some military and law enforcement experience can help individuals transition into private-sector security management positions, not all training and conditioning from these career paths prepare applicants to flourish in private-sector careers. Their past experience, training and education should be relevant to your position.

Qualifications
The most appropriate candidates will often have a mix of relevant experience, education and certifications.

Experience
Relevant experience should include:
• A minimum of five years of successful security management in a similar type of private-sector organization
• In-depth knowledge of the many aspects of security management (risk management, emergency management, electronic security system design, physical security, etc.)
• Familiarity with business management concepts and customer service
• The ability to partner with other division heads
• Strong leadership and mentoring skills
• The ability to develop and implement policies and procedures

Many of the best private-sector security directors have worked at multiple levels (assistant manager, manager, etc.) within the security management field before taking a senior-level position (director).

Given that most JCC locations have high traffic and diverse groups of people coming and going at all hours of operation, viable applicants should have security experience within similar environments (shopping mall, hospital, school district, high-rise office building, event security, major sporting venues, etc.).

Education
An undergraduate or graduate degree in security management is preferable.

Certifications
Certifications from an organization such as ASIS International would be good indicators of appropriate levels of competency. For example:

The Physical Security Professional (PSP®) credential provides demonstrable knowledge and experience in threat assessment and risk analysis, integrated physical security systems and the appropriate identification, implementation and ongoing evaluation of security measures. Those who earn the PSP are ASIS board-certified in physical security.

The Certified Protection Professional (CPP®) credential provides demonstrable proof of knowledge and management skill in seven key domains of security. Those who earn the CPP are ASIS board-certified in security management. A CPP certification encompasses the Physical Security Professional (PSP®) credential.

Basic Interview Questions
Using your job description as an outline, choose relevant questions from the list below and request that the applicant describe his or her experience:
• How will your education, certifications and experience help to facilitate the goals and objectives described in the job description?
• How do you intend to advance your knowledge in the security management field?
• Do you have any applicable certifications in the security management field?
Ask the applicants to explain their experience in the following areas:

- Management and budgeting
- Facility access control and visitor management
- Customer service
- Working with other business groups and senior management
- Threat analysis and management
- Mentoring staff members
- Crisis or emergency management
- Liaisons with law enforcement
- Electronic and physical security systems
- Developing security policies, standards and guidelines
- Program auditing (policies and systems)
- Guard force management
- Investigations
- Security assessments and report writing
- Security training

Lessons Learned

As you consider hiring a security professional, take the following points into consideration:

- Do not advertise for a position or interview candidates until a job description has been formalized and approved.
- Do not let impressive experience in areas outside of your job description influence your decision.
- Do not underestimate the amount of time and resources it will take to educate a candidate in an area in which he or she is unfamiliar if that area is a key requirement in your job description.
- If you utilize security technology as part of your protective strategy, ensure that prospective candidates have experience in the systems and components utilized at your facility.
- Understand that security professionals require ongoing education to acquire or maintain security management and certifications.
- Security management certifications can often assist you in acquiring insurance.
- If you hire a security professional who was not a police guard, do not assume that he or she will not be an efficient law enforcement liaison. Working with and acquiring assistance from law enforcement does not require a past law enforcement career.

Hiring a Security Consultant

The above recommendations and guidelines will also be of assistance in hiring a security consultant. It is critical to develop a scope of work for the project and to define deliverables, time frames for different stages of the project and a payment schedule. The consultant should sign a certification of adequate insurance coverage and your non-disclosure agreement. Review documentation concerning experience in relevant areas. If you will also utilize sub-contractors, conduct the same level of review for each subcontractor. Conduct a background investigation on the company and all persons who will be on-site and/or handling your data.

Note that consultants need only be proficient in the areas of work for which they are hired. If you anticipate multiple projects over a short period of time and prefer that one consultant complete all projects, he or she should have an appropriate level of competency in each area.

Questions and Calls to Action

1. Your organization has decided to hire a security professional. How will the development of the job description take place, and who will develop it?

2. Who will supervise the security professional? What do they know? What training do they need to be able to effectively supervise this person?

3. The security professional that oversees the building or campus where the JCC is located is not an employee of the JCC. What practices have been set up to make sure JCC security needs are correctly addressed by the security professional?
SECTION L

VISITOR MANAGEMENT/
UNAUTHORIZED PERSON ON PREMISES
Visitor management is a vital element of a good security program. You should always know and approve of all persons accessing your facility, including business visitors, vendors, contractors, prospective members, tenants’ visitors, delivery personnel, JCC staff, guests, etc. Government photo ID should be used to authenticate the individual. In some cases, students without government ID can use a school photo ID. Your visitors’ IDs should be also scanned (scanning allows you to mask sensitive areas of their ID), and you should keep a record of their visit for a minimum of two years.

Guidelines for Visitor Management

Your visitor management process should direct all individuals without JCC ID to your main reception area or another area designated for processing. Once processed, they should be issued a visitor ID that should be displayed throughout their visit and returned when they leave your facility (even if they are planning to return).

Personal guests should be approved by each staff member’s manager prior to their arrival. Visitors should never be granted access without having their identities verified and having their hosts informed of their arrival. Staff members who receive visitors should be aware that they are responsible for reporting visitors who are announced upon arrival but do not then meet them for their scheduled appointments. Management should be alerted about visitors who check in at the lobby but do not reach their stated destination. Depending on your facility and the visitor’s destination, an escort may be advised.

Your visitor ID tag should be unique and difficult to copy. IDs should be unique for each day of the week (and varied regularly) or time-sensitive. Preferably, it will be easy to identify once they are expired. Visitor ID tags should include a photo that is clear, appropriately sized (at least 2 by 2 inches) and recognizable (a recent photo that is a good representation of the visitor). Pictures can be rapidly taken and stored for future visits the first time the visitor accesses your facility and/or scanned from a driver’s license. An electronic visitor management system can assist in managing this process. One system can scan driver’s licenses and/or take photos; enter information into a database; print credentials; record duration of visit, person visited, and visitor’s organization; and maintain a historical record of the visit. Systems can also include a “watch list” feature that will notify you if the individual is banned from your facility, has a criminal record and/or is listed in a sex offender database. Many visitor management systems allow staff to preregister their own visitors. This will minimize the time required at the front desk, ensure accuracy and expedite the entire process.

The physical layout of your facility, as well as possible tenants and their access points, will need to be addressed. If you supply space to tenants (physical therapy, external organizations, etc.) who service non-members who access their offices through your facilities, they should also be processed through your visitor management system. If tenants have their own entrance and exit, but fire egress doors or other interconnecting doors will permit access to your JCC, access points should be alarmed and under video surveillance, and signage indicating that an alarm will sound if doors open should be placed appropriately. Consider having tenants’ visitors escorted to and from their destinations by tenant staff. One of the easiest ways for a bad actor to access your facility without authorization would be to make an appointment with a tenant whose clients have unfettered and/or unrecorded access to your facility.

When national vendors (Verizon, Xerox, FedEx, etc.) require access to your facility, they should use government photo ID (driver’s license). Some national vendor employees prefer to show company ID, which can be easily copied and/or modified. National vendors’ management supports their employees showing both government and company photo ID. An uncooperative vendor (i.e. one who refuses to show government ID) should not be permitted access to your facility. If their service call is mission-critical to you, place them under constant security escort.

Where possible, personal food delivery staff should not be granted access to the facility.

When hosting on-site events, all staff (setup personnel, photographers, waitstaff, lighting crew, event coordinators, delivery personnel, additional security guards, etc.) associated with the event should go through the same visitor management process. This should also include all guests, speakers and media personnel.

Visitors who leave the premises should be required to return their visitor IDs. If they intend to return later that same day, they can notify reception staff as they leave, and their original ID card will be returned after they go through the same management process (check ID and call visitor host for approval).
Conclusion for Visitor Management

Prior to enhancing or implementing a new visitor management program, all staff should be made aware of the new process and their responsibilities. Each JCC is unique in design and functionality. Each facility will have to evaluate its own visitor management security needs and develop a program that balances security and operational needs.

Guidelines for Unauthorized Person on Premises

In a JCC environment, an unauthorized person could be found accessing your facility for a number of reasons. Someone interested in becoming a member could unknowingly wander past your reception desk, a high school student could attempt to avoid security to meet friends on the basketball court or a criminal could gain undetected access in order to steal from your members. Unauthorized access could also involve a sex offender, an anti-Semitic actor, workplace violence, a custody issue or someone who is testing your security with a view to committing a heinous act. The focus for this section is not so much to determine an intruder’s actions or motivations, but rather on how to prepare for an unauthorized person on premises. What is involved in a response? What are staff responsibilities? This may not happen often, and most events will probably be minor, but unauthorized access could result in a serious issue. The presence of an unauthorized individual should be considered a pre-event indicator and should be acknowledged, efficiently evaluated and appropriately acted upon.

Key components to prevent against unauthorized entry include:

- Serious consideration of all incidents of unauthorized access
- Good security controls to limit opportunity (look like a hard target, be a hard target)
- A well-trained staff that can identify unauthorized persons (promote a security awareness culture through training)
- Rapid reporting of all observations (staff knows their responsibilities)

In order to identify the severity of an event, establish a quick and effective evaluation process. Develop a written response plan and train staff on how to search for unauthorized persons and quickly utilize security equipment and the camera system. Take prompt action, keeping in mind that responses can vary greatly. There are many situations between something that “turns out ok” and a terrorist attack. Your facility may have to lock down, move people to a more secure area within the building or evacuate. The event may require a response by your security guards, management and/or the local police department. Someone should always be on-site who has the authority to immediately call the police. Sometimes, however, a stern talk with the rule-breaker is all that is necessary.

The final and crucial step in a reported event is to record all pertinent information into a file that might be used later to help detect or confirm future suspicious behavior.

In conclusion, staff should know their responsibilities, including how to report unauthorized persons. Without direction, staff may not recognize this exposure or feel obligated to report it. You cannot manage a potential threat without knowing its nature or frequency. Based on the information provided by your staff, you will determine whether a threat requires a quick and appropriate response to a dangerous situation (someone photographing your security equipment or children at play) or a timely response to a rule-breaker (one member letting another member in through a back door). Without a known plan for reporting, a quick and appropriate response is unlikely to occur. Planning and training are the two key elements of a successful security program.

Conclusion

The period of time between your first observation and the need to respond could be very short. It is very important to identify a potential problem as soon as possible. Often, a facility will have a state-of-the-art security system that is properly installed and capable of promptly detecting a problem, but staff is unaware of the system’s functionality, does not know how to use the system’s components or is not fully monitoring cameras and alarms. If staff does not know how to perform assigned duties and/or fails to understand the importance of diligence, the best physical security programs can fail.
SECTION M

SUSPICIOUS MAIL IDENTIFICATION AND RESPONSE
SECTION M.
SUSPICIOUS MAIL IDENTIFICATION AND RESPONSE

Staff who handle mail or packages (U.S. Mail, UPS, FedEx, special deliveries, hand deliveries, etc.) should have the training necessary to identify and respond to suspicious packages and letters. Because those who would utilize these delivery mechanisms to threaten or harm your organization continuously alter their techniques and procedures, this section will include generic concepts for identifying and responding to suspicious mail. Up-to-date information and training materials relating to identifying and responding to suspicious packages is available from the United States Postal Service, the Department of Homeland Security and other law enforcement agencies. The U.S. Post Office will provide on-site training sessions for your staff upon request. This is excellent training and your organization should take advantage of the opportunity to send designated staff members.

Because of the evolving nature of this threat, it is always best to check with the above agencies for updated information.

Identifying Suspicious Mail or Packages

Generally, be aware of letters or packages that have suspicious traits.

Suspicious traits include, but are not limited to:

- Handwritten or poorly typed addresses
- Incorrect or misspelled titles
- Misspelled names or misspelled common words
- Title, but no name
- Restrictive markings: “Confidential,” “Personal” or “Do Not X-Ray”
- Excessive postage
- No postage
- No return address
- A city or state in the postmark that does not match the return address
- Unusual, unverifiable or nonsensical return address
- “Handle with Care,” “Don’t Shake or Bump” or similar instructions
- Mailed from a foreign country
- Foreign writing, postage or return address
- Oily stains, wet areas, openings, strange odors, discolorations or crystallization on wrapper
- Excessive weight
- Lopsided, rigid or uneven packaging
- Protruding wires or tin foil
- Ticking, vibration or other sound
- Excessive securing (tape or string)
- The presence of small bulges of powder or granules
- Anything unusual, not normally sent to your location

Response to Suspicious Mail or Packages

- Notify your supervisor or security.
- Clear the immediate area of all persons and keep others away.
- Do not open the letter or package (or do not open any further) or empty its contents. Do not shake it.
- Do not show it to others.
- Leave the letter or package where it is or gently place it on the nearest flat surface; do not jostle it.
- If it is leaking, do not try to clean up the leak.
- If possible, gently cover the letter (use a trash can, article of clothing, etc.).
- Shut down all equipment in the immediate area, including HVAC systems (heating, ventilation, fans and air conditioning).
- Evacuate the area and close the door to the space containing the suspicious letter or package. Cover the threshold area under the door with a towel or a coat if possible and section off the area (keep others away).
- Restrict access to floors above and below and areas on all four sides of the affected area.
- Ensure that all persons who have touched the mail or package wash their hands with soap and water.
- List all persons who have touched the mail or package and/or were in the general area. Include all contact information for these individuals. Have this information available for the authorities.
- Direct affected people to a designated area away from the substance to await further instruction.
SECTION N

ADDITIONAL RESOURCES
LINKS TO ADDITIONAL RESOURCES

No list of identifiers and responses to suspicious mail or packages can be all-inclusive. The documents and training materials found at the links below will assist you in developing a plan for your location. Keep in mind that if a dangerous item is identified, you will have to evacuate your facility; procedures for this should be included in your overall security and crisis management plan.

**Bomb Threat Checklist**
tripwire.dhs.gov/IED/resources/docs/DHS%20Bomb%20Threat%20Checklist.pdf

**Bomb Threat Stand-Off Card**
tripwire.dhs.gov/IED/resources/docs/DHS-DOJ%20Bomb%20Threat%20Stand-off%20Card.pdf

**Bomb Threat Management Guidance Quad-Fold**
tripwire.dhs.gov/IED/resources/docs/OBP_DHS_DOJ_Bomb_Threat_Guidance.pdf

**Bomb Threat Management Video**
tripwire.dhs.gov/IED/resources/jsp/ucfVideo.jsp

**Suspicious Mail or Package Indicators**
about.usps.com/posters/pos84.pdf

**DHS Response Checklist**
hsema.dc.gov/sites/default/files/dc/sites/hsema/release_content/attachments/20982/Susp_Mail_DHS.pdf

**DHS Safe Mail Handling Procedures**
osec.doc.gov/osy/PDF/SafeMailing.pdf

**DHS Best Practices for Safe Mail Handling**
fbiic.gov/public/2010/nov/safe_Mail_Handling.pdf

**Bombing Prevention Lanyard Card**
tripwire.dhs.gov/IED/resources/docs/Bombing%20Prevention%20Lanyard%20Cards%20(Unlined%20Version).pdf

**Bomb Making Materials Awareness Program (BMAP) Video**
tripwire.dhs.gov/IED/resources/jsp/bmap.jsp
PREVIOUSLY RELEASED SECURITY BULLETINS

**Security Bulletin 1, May 2017**
Executive Summary—Foundation for Establishing a Security Mindset ................................................................. 90

**Security Bulletin 2, June 2017**
Target-Hardening and Early Detection (Training Curriculum Included) ................................................................. 96

**Security Bulletin 3, June 2017**
Security for Summer 2017 ........................................................................................................................................ 103

**Security Bulletin 4, June 2017**
Emergency Response Plans and Providing Safe Havens .......................................................................................... 107

**Security Bulletin 5, August 2017**
Protest Rally Preparedness for JCCs ..................................................................................................................... 112
EXECUTIVE SUMMARY

May 2017

Foundation for Establishing a Security Mindset

This report, and two subsequent reports, provide suggestions, recommendations, observations, scenarios and training templates around security for JCCs and camps to use during summer camping activities. The documents introduce four high-level strategies into which security activity falls: looking like and being a hard target, early detection, appropriate response plans and providing safe haven. It also elaborates the necessary preconditions ("foundations") for a security mindset.

JCC Association is mindful that the pace of review, consideration and uptake of the information contained herein lies with the individual JCC and camp. Some items are immediately actionable, while others will require more time—and possibly more resources. Over the long run, the effort is to create a more sophisticated appreciation and incorporation of a security mindset into JCC and camp activity.

The information will be released in three parts. Part 1—this document—introduces the four strategies and the foundation for establishing a security mindset. Part 2 focuses on the first two strategies, and Part 3 introduces the last two strategies. This will allow directors to read and absorb the information at the pace they prefer. Each part will address specific aspects of security preparedness. The reports are written to help JCC camps prepare and respond more effectively to threats and attacks and have two specific goals:

- To provide clear explanations and examples of practices for your camps to adopt, and
- To help you achieve a more sophisticated understanding of security as an ongoing discipline.

PREFACE

Off-Site Day and Overnight Camp Security Strategy: Framing the Context

Every camp director knows that the physical safety and well-being of the camp community is always the first priority. JCC camps have a long and effective record of providing safe and secure environments for their programs. Recent events in the JCC world and around the globe are stark reminders that the protection systems JCCs have in place to guard against typical threats (angry ex-employees, couples in nasty custody disputes, vagrants and local hoodlums) are insufficient when facing anti-Semitic extremists looking to make a statement. JCCs today face greater risk factors and therefore must upgrade their ability to protect the members of their communities. The recent bomb threats make it very clear: Now is the time for every JCC to review and revise its security and emergency management strategy. Every JCC camp should consider the threat level for summer 2017 higher than that of the previous year, even if your JCC did not experience any incidents or threats of violence.

The information provided in this document is designed to deliver helpful information on the subjects discussed. The information and references shared are the expert opinion of Paul DeMatteis, Global Security Risk Management, LLC, an independent consultant hired by JCC Association of North America. This document is not an alternative to local law enforcement protocols and advisement. The information within this document is meant for JCCs of North America and independent camps affiliated with JCC Association of North America. This document should not be copied, shared, or otherwise distributed outside the original intended recipients.

© JCC Association of North America, 2017
Introducing the Four Strategies

There is no single thing that ensures the safety and security of any facility or campus. Rather, it is the cumulative impact of proper planning and implementation in four primary areas that yields the best outcome:

1. **Look like and be a hard target.** People looking to do harm will choose the easiest target. If it looks hard to gain access to your JCC, a potential perpetrator will turn away and look for something easier.

2. **Early detection systems.** The sooner you can identify a “bad guy,” the more time you have to respond; each extra minute provides an extra margin of safety. Identifying a threat at the entrance to the parking lot rather than at the entrance to the building can mean lives saved.

3. **Appropriate response plans.** Having plans for the types of threats you anticipate is merely the first step. Ongoing staff training, drills and simulations are integral to the success of any plan.

4. **Providing safe haven.** Deterring a threat from entering the JCC is a goal but having multiple locations within the JCC to offer shelter if necessary while waiting for law enforcement to arrive is essential. Your law enforcement liaisons and partnerships are critical components that must be proactively fostered throughout the camp season.

**FOUNDATION FOR ESTABLISHING A SECURITY MINDSET**

**Understanding the Hostile Act and Actor**

A hostile act is an attempt to use deadly force on one or more individuals. It can include an active shooter, a terrorist attack, a child custody issue, a criminal act turned violent or any other act during which there is an attempt to use deadly force. Such acts can be, and typically are, completed within four to seven minutes or less. You must be prepared in advance to manage such an incident, if there is hope of mitigating damage and loss.

Time is the enemy of a hostile actor. They know that once we are aware of them (breaching a fence or entry, an explosion, or a shot fired), they have a very limited amount of time to complete their mission. The more time you have, the better you will be able to limit the impact of an event. Failure to identify a bad actor before a killing or otherwise violent spree dramatically increases his ability to harm a larger number of individuals.

Hostile surveillance, thought to have been conducted in all known attacks, is a tool our adversaries use to ensure their success. Detecting hostile surveillance provides us with an opportunity to become aware of hostile actors’ interest and report it to law enforcement. Identifying hostile surveillance is the best course of action because the event might possibly be prevented if it is recognized and quickly reported to law enforcement. In a public area this might be difficult, but on private campgrounds there are many opportunities to identify individuals who do not belong there and who are focused on observing campers and/or security procedures and protocols. Someone watching how we respond to a trespasser, bomb threat or suspicious package can provide a great deal of valuable information to our adversaries.

The information provided in this document is designed to deliver helpful information on the subjects discussed. The information and references shared are the expert opinion of Paul DeMatteis, Global Security Risk Management, LLC, an independent consultant hired by JCC Association of North America. This document is not an alternative to local law enforcement protocols and advisement. The information within this document is meant for JCCs of North America and independent camps affiliated with JCC Association of North America. This document should not be copied, shared, or otherwise distributed outside the original intended recipients.

© JCC Association of North America, 2017
Camp Security Management
An effective security plan relies on three basic management principles:

1. **Clearly defined roles and responsibilities.**
   As in any business process, there must be a structure established for security that outlines leadership, accountability and areas of responsibility. It should be clear to all who is the head of security (most likely only one of the many areas of responsibility for that staff member). That individual must accept the responsibilities, be accountable and dedicate the necessary time to effectively manage security. If security responsibilities are decentralized among multiple persons who have fractional responsibilities without appropriate direction and coordination, your protective strategy will be flawed. In some cases, it will appear to be working effectively, but if tested under the duress of an actual event, the lack of coordination will become clear.

2. **Compliance**
   It is also important to ensure that senior management supports the security function and that security becomes an integral part of the camp’s culture. Three things that will unintentionally jeopardize your security program are:
   • Ignoring risk
   • Ignoring unauthorized exceptions
   • Providing special privileges

   Ignoring security risks can lead to serious security events. A number of crime studies have shown that after a security incident, the investigative process identified a number of people who were aware of the risk and chose to simply ignore it. The main reasons they gave were that they were uncertain about management’s interpretation of their interference and/or that they feared they would be perceived as criticizing established policies. Additionally, your security policies should include a procedure to officially authorize needed exceptions to security protocols, including who can authorize them.

3. **Documentation**
   An effective security plan exists only as a real-time document, one that must be regularly reviewed and updated. If you choose to use some of the recommendations within this document and incorporate security monitoring counselors, security guards and/or off-duty police guards, that alone is insufficient. Your written security procedures, guidelines and reporting structure should be clearly defined. Law enforcement and security professionals, you work with will ask you for such procedures; without such, the good professionals are unlikely to want to work with you, and the inexperienced ones (like security monitoring counselors) will fail without them.
**Developing and Maintaining Police Relationships**

Keeping close ties with local and state law enforcement is critical, especially since you are only operational for a short period of time. Each year, before camp starts, you should meet with your local police chief and, if applicable, the guard in charge of your local state police unit. You can call to ask for a meeting, which will likely last 30 minutes or so. For some of you, this meeting will be a first-time visit to establish a working relationship. To assist in this meeting, below are topics worth discussing:

1. Introduce your camp and management team and offer a copy of your camp brochure. Local law enforcement is probably aware of the recent threats against JCCs, but they are still worth mentioning. Even though the most recent threats were hoaxes, voicing your concern regarding copycat events and other violent crimes committed against JCCs and the community as a whole is a legitimate topic for discussion.

2. Provide a list of 24-hour contact numbers.

3. Invite law enforcement to your camp; it is always better if they have the opportunity to review the layout of your facility and campgrounds, including all points of access, before an emergency. If possible, they might even provide you with a crime prevention assessment.

4. Provide an updated copy of the camp’s security plan. It should include an updated map of the facility.

5. If your campgrounds are near other police districts, ask law enforcement if they maintain contact with other police departments in the area. If you border multiple jurisdictions, it is a good idea to reach out to each of the nearby law enforcement departments. Getting warning of nearby camp-related crime or suspicious activity is critical.

6. Ask law enforcement to share any suspicious activity information with you. You will not need sensitive case information, just general information on the threat and a description of any vehicles or individuals that could be involved.

7. Ask if they have a crime prevention or public affairs guard, who could be very effective in helping you throughout the summer.

8. Ask about response time. This is always a sensitive question. Depending on location, time of day, day of week, patrol patterns and staffing, response time can vary greatly. Find out how much assistance they can supply during an emergency, as some rural police departments might not have the resources to handle a large-scale emergency at your site. Again, remember that state police could also play a major role in emergency response.

9. Inquire about hiring off-duty police guards. There could be some preliminary paperwork required. You can also inquire about retired guards who might be interested in working at the camp (security, coaching, etc.). It is beneficial to have such information for future planning purposes.
10. Ask if they offer training sessions useful to the camp. If not, you can ask if there are any provided by the county and/or state. Training programs can include such topics as active shooter, crime prevention, gun safety, first aid, etc.

11. Ask if they can provide you with an overview of local crime (violent crime, sexual predators, hate-related events, etc.). This can be just general information. Some departments have this information online.

12. Ask if they intend to hold a joint meeting with other camps in their jurisdiction. Creating a network to share critical information is definitely worth the time it takes. If they do not, suggest hosting one at your location.

13. Ask for one senior guard to be assigned to you as your liaison with the department (it might be the police chief).

14. If they have not provided detailed contact information, ask for a directory of cell phone numbers (the chief, shift captain, dispatch, etc.).

Please do not consider this list of agenda items exhaustive. Each camp has unique concerns and questions, and it is your responsibility to articulate them. Do not be shy; law enforcement officials are generally happy to contribute to your ongoing security education.

Of course, a yearly meeting is necessary but not sufficient for developing a close relationship. It is also worth considering the following:

- Where it would not raise undue concern on the part of your camp community, invite local law enforcement to any interesting events taking place at camp.

- Invite local law enforcement to use your facility for training exercises prior to camp opening. You might also want to provide some sort of off-season usage for first responders.

- If the camp is owned and operated by a JCC, offer law enforcement and other first responders complimentary membership. The more familiar they are with the facility, the better they can help in an emergency. Also, an ongoing presence of law enforcement vehicles and personnel provides a visual deterrent.

Many of you may already hold periodic meetings with local law enforcement as part of an ongoing relationship. In that case, you likely will have dealt with these issues already. However, a review of the list is well-warranted for any additional items not covered previously. Furthermore, given the events of the early part of this year, you may find local police more attuned to your security needs.
JUNE 2017: BULLETIN 02
TARGET HARDENING
and
EARLY DETECTION
(Training Curriculum included)
TARGET HARDENING and EARLY DETECTION
(Training Curriculum Included)

INTRODUCTION

The first security bulletin presented four security strategies for camps, as well as JCCs: target hardening, early detection, appropriate response plans and providing safe haven.

This second bulletin describes target hardening and early detection more comprehensively. Target hardening addresses three topics: three elements of basic security, daily site inspections and basic security concepts and controls. Early detection addresses four topics: the elements of early detection, building staff awareness, a sample security training agenda for all staff (located at the end of this document) and suggestions to augment staff awareness with dedicated security personnel that, if not feasible for summer 2017, can be considered for future summers.

STRATEGY 1: TARGET HARDENING STRATEGY

People looking to do harm will choose the easiest target. If it looks hard to gain access to your camp or JCC, a potential threat will turn away and look for something easier.

Basic Security Elements

The following three elements are critical to basic security controls:

1. **Leadership.** An effective security program requires constant leadership, ongoing management, a common-sense approach to risk and mitigation strategies, clearly defined areas of responsibility, accountability and everyone’s participation. As indicated in the first bulletin, one person needs to own the security function at camp, even if that function is just a part of his or her responsibilities.

2. **Strategy.** An effective protective strategy balances acknowledged risks and threats and provides mitigation plans, training, awareness and emergency response protocols. Its design and implementation depend upon the physical environment, local culture and ordinances, whether there is a need for temporary or permanent solutions and the availability of capital and manpower, among other things. These and any other special conditions must be considered to achieve a balance in your program.

3. **Controlled access.** Effective security controls allow only authorized persons on-site and provide alerts of potentially unauthorized access.

There is no one single solution for providing effective security (electronic, procedural, armed security, capital expense, staffing, etc.) for all camps and all settings. Awareness, following procedures and using controls will maximize your protection strategy. Complacency, making exceptions, ignoring your instincts and failing to utilize your physical or electronic systems effectively will greatly diminish your program.
Site Inspections

Daily site inspections are critical. They can act as a great deterrent, helping to identify safety and security issues before they become a problem. The daily inspection should include:

1. Primary and secondary entrances
2. The full perimeter of your property
3. Trails that access your property
4. Play areas and common buildings
5. Areas that would be suitable for hostile surveillance
6. Areas where trespassing would likely occur, based on your past experiences

Inspection routes and times should vary from day to day. Keep inspection logs listing areas inspected and exceptions noted.

Inspection personnel must have communications equipment and should report any unusual or dangerous conditions immediately. Depending on the size and complexity of your grounds, this might require multiple individuals and possibly a vehicle. Daily secondary inspections should be conducted at different times and in different directions so as to avoid establishing a pattern.

Basic Security Concepts and Controls

1. The main entrance, and any secondary vehicular entrances, should they exist (and if possible, not) should have the same level of controls. Walking trails that cross the camp’s boundaries should be marked as such, private property signs should be posted and rudimentary controlled access (wooden gates, chains) put in place.
2. Place a security gate at the main entrance driveway. The gate and surrounding area should be well-lit to allow proper processing. The gate should be sturdy enough to deter a vehicle from attempting unauthorized access. The gate should close after each authorized entry. The best practice is to use a motorized gate that can be remotely operated. Areas to the side of the gate should not allow vehicles the ability to bypass. This can be accomplished by releveling the terrain, installing appropriate steel and masonry columns and/or putting obstacles (boulders, etc.) in the path of an unauthorized vehicle.
3. Place a security booth with a full view of approaching vehicles near the main gate. It should be equipped with electrical power, interior and exterior lighting and communications equipment (walkie-talkie, phone, emergency notification button, etc.). If the facility is equipped with a camera system, the security booth should have the ability to monitor cameras. (Only select cameras should be permitted for display at this location, i.e. cameras that would not jeopardize your overall security if observed by an unauthorized person.)
4. Install a barrier (bollards, etc.) in front of the security booth and in the direction of approaching vehicles. This provides protection for the booth occupant.
5. Consider a video surveillance system for the main gate and secondary vehicle access points. Cameras should also be considered at secondary entrances and exits, at waterway access points (if camp is on a public lake and cameras must be on camp property), along key walking routes onto your property, along main internal roads and near buildings and general activity areas. All cameras should be monitored from a central location and be capable of remote viewing via a secure network.
6. Fences act as a deterrent. Depending on the camp’s location, size, terrain, public access, adjacent unsecured property lines and local codes, consider a fence to restrict access. Fencing helps distinguish between an intruder climbing over the fence and someone merely taking a shortcut across your property. Knowing the difference can provide you with additional time to initiate your emergency action plan.

1. Your maintenance team can install a number of cost-effective and high-quality cameras. Some of the new cameras are battery- and/or solar-powered, equipped with video motion detection and capable of storing video on a local chip. If you have Wi-Fi or cellular service in the area, it can be used for remote video storage and monitoring. In some applications, running a temporary fiber-optic cable is also an effective solution for remote monitoring. All cameras should be recorded for a minimum of 30 days, at a minimum of 15 frames per second. Cameras should also be monitored from within the camp whenever the camp is occupied. All wireless video transmission should be secure (encrypted).

7. Play areas near public and private access roads need protection from cars and trucks used as weapons. You can achieve this by installing anti-ramming devices, releveling your terrain, creating a masonry wall, placing obstructions in the path of approaching vehicles (boulders, vehicles, etc.). Identify structures that would make good shelter-in-place locations. Ideally, they should be spread across the campgrounds. They can be bathrooms, auditoriums or meeting rooms. It is recommended that shelter-in-place facilities provide a minimum 10-minute barrier from an armed intruder. (More detail on providing safe haven will be in bulletin #4).

The above are general baseline security controls not specific to your facility. Your facility has unique conditions that likely have not been addressed. Meeting with local law enforcement and/or independent security consultants, as well as conducting your own review and assessment, will suggest additional controls needed at your facility.

Please remember that temporary solutions can be used in the interim as potential threats are evaluated and more permanent solutions are developed and implemented. Temporary solutions might include staffing an entrance in the absence of a gate or security booth or parking a vehicle or other obstacle to limit vehicular access.

STRATEGY 2: EARLY DETECTION STRATEGY

The goal of early detection is to provide as much warning as possible of a threat. Each extra minute provides an additional margin of safety because it gives you more time to respond. This can mean lives saved.

Elements of Early Detection

A proactive security program provides identification of early indicators of a potential problem and a prompt response, reducing (although not eliminating) the risk and impact of a hostile event. If identified in the early planning stages, law enforcement might be able to neutralize the problem before the plan can be executed. In real terms, early detection is the first layer of effective security.

An effective early detection plan involves many elements, including:

1. Building staff awareness
2. Collaboration with law enforcement
3. Monitoring current events
4. Sharing information with other camps and JCCs
5. Forming alliances with other camps
6. Regular camp inspections
7. Security training for staff
8. Regular exercises and drills

Key among early detection strategies is building staff awareness.

Building Staff Awareness
Camp staff at all levels of responsibility should know that they share responsibility for early identification of threatening acts. It is the camp’s responsibility to provide the necessary training, which requires a minimum of one to two hours of security awareness training designed for a camp environment and customized for your location. Today’s young adults have had many years of school-based active-shooter training. This type of training should be empowering. A sample training agenda for all staff is on the next page.

Dedicated Security Personnel
Camps may choose to have dedicated security personnel on the campgrounds. While this provides an additional layer to the early detection strategy, it alone is not sufficient without building staff awareness around security. That said, trained personnel, such as private security, off-duty police or more highly trained “security counselors,” are likely to provide a keener eye to the observation part of early detection, better evaluate specific situations and act more decisively and rapidly.

**SAMPLE SECURITY TRAINING CURRICULUM FOR ALL JCC CAMP STAFF**

This sample training curriculum is designed to enable camp staff to recognize suspicious activity, identify early indicators of hostile surveillance or early detection of hostile actors on the day of an attack, and take immediate action (to be customized to suit your camp’s individual needs). The one- to two-hour training module should be broken down into 20-minute blocks.

**Section 1 - The Basics**

a. Introduction to camp history, campgrounds, access points and hiking trails (if not covered in other staff training or documents).

b. Introduction to security awareness

Definition: Security awareness is a set of practices shared by members of an organization or group regarding the protection of the staff and assets of that organization. Security awareness requires maintaining specific knowledge and a specific attitude. Being security-aware means accepting responsibility for preventing or mitigating damage from a potential hostile actor. A security-aware camp provides its staff with the tools to recognize suspicious activity and report it to those in charge of security. This keeps the camp community safe.
Section 2 - Observing

Knowing what constitutes suspicious activity is a first step. Some typical indicators are listed below. Please know this list is not exhaustive; if you have had incidents on your campgrounds or have been notified by law enforcement of any local issues, it is recommended that you add relative indicators to this list.

a. Watchers
   1. Someone watching the campers at play; they might even look enthusiastic about the activity
   2. Someone watching and/or taking pictures of campers, buildings, front gate, other security controls and/or during evacuation drills, etc.
   3. Someone sitting in a wooded area watching the campgrounds (on or off your property)
   4. A drone flying over or near the camp
   5. Someone observing your camp from a road, hiking trail or neighboring property
   6. If water-accessible, someone monitoring your property or security protocols from a boat
   7. Someone asking for directions at the main gate or along the property line who does not appear to fit in

b. Strangers and Strange Behavior
   1. Someone you don’t know carrying bulky and/or heavy bags
   2. Someone you don’t know looking angry and/or annoyed
   3. While off-site, anyone showing unusual interest in your presence and/or inquiring about your camp or its security controls
   4. An individual hiking through your property
   5. Someone on your property asking for directions for a delivery or doing a repair
   6. Individual carrying equipment inconsistent with camping or hiking activities, military-type equipment, a GoPro, hunting gear during non-hunting season

c. Anomalies
   1. A locked door to a room in which hazardous chemicals (chlorine, gasoline, propane, etc.) are stored is found open
   2. Any indicators, including unauthorized campsites, that unauthorized persons might have been on your property
   3. Finding trail cameras on your property
   4. Suspicious calls, inquiries about security or emergency management or opinions on sensitive matters
   5. Something new in an area or in a building that could indicate a suspicious actor
   6. Something missing that might indicate an unauthorized person on your property
   7. Something moved to enable an individual to reach an upper window

Any of these indicators could suggest a hostile act, but also could be harmless. However, individuals can analyze information uniquely and combine innocent observations into a suspicious pattern. All incidents must be evaluated and taken seriously; immediate evasive actions might be warranted until the situation has been clarified. For each observation, camps need to decide on and instruct and train staff in a preferred course of action. Regardless, all observations should be reported to a central person or office, and all observations should be recorded in detail.
Section 3 – Making Decisions

Where an observation may not conform to the preferred course of action, there are four steps in making a security decision:

Observe, Orient, Decide, Act (OODA)

1. **Observe**: See list above
2. **Orient**: Ask, “Does this make any kind of sense?” Is the observation consistent or inconsistent with normal activity, based on the staff person’s knowledge of camp, including what he or she has been trained to take as the preferred course of action?
3. **Decide**: If the observation represents a threat, what level threat? What response strategy should be initiated?

   The options include:
   a. Continue normal activity but notify security leadership as soon as possible.
   b. Interrupt the current activity to notify security leadership immediately.
   c. Interrupt the current activity to either: Avoid (escape), Barricade (shelter in place) or Confront the threat (fight). Obviously, emergency escape routes and shelter-in-place locations must be designated in advance. Seconds and minutes count.
4. **Act**: Carry out the decision

Section 4 – Questions and Answers

The question and answer section is a critical component. Participants should be encouraged to ask questions as a whole group, not individually after the session. If no one has questions, you should promote their participation. Generally, after a few people ask questions, the process starts to take off.

Below are some general starter questions:

a. Has anyone here had this type of training in the past?
b. If you see something suspicious, will you feel comfortable reporting it?
c. What is the easiest part of this process?
d. Is there any one aspect of this process with which you feel you will have difficulty?
e. Do you understand why, in today’s world, security is everyone’s responsibility?

Often, participants’ questions will reveal their level of understanding of the material and their commitment to this new responsibility. Responses to their questions will help them to determine their level of commitment.

Be prepared to answer all the “what-if” questions. Everything presented should make good common sense.

Participants should feel empowered with this new information and training. Continue until all questions have been answered.

After this initial training session, weekly updates should be presented during all levels of staff meetings. Such updates would include a briefing on any recent local or regional activity that could impact your camp. If any suspicious activity is noted, your security posture must be immediately re-evaluated, and appropriate measures taken.
June 2017  
Security for Summer 2017

The series of bomb threats against JCCs in early 2017 jump-started a heightened awareness of the importance of effective security protocols. JCCs became more adept at responding to phone and email threats, connecting with local law enforcement, refining their emergency procedures and establishing a more sophisticated communication practice with their constituencies and the media.

During this extended crisis, funders interested in aiding JCCs and camps with regard to security volunteered their support. This allowed JCC Association of North America to further help its constituents beyond the work that its consultants were already conducting.

JCC Association understands that the timing of this effort came too late to have a significant impact for summer 2017; normally, suggestions would have been made last fall, prior to the current year’s budget cycle and with enough lead time for thoughtful implementation. Still, security is an ongoing concern and we believe many of the suggestions below are achievable in summer 2017. JCC Association hopes this abbreviated overview will be helpful in shaping camps’ thinking about security for this season.

CAMP SECURITY 2017

1. All camps should have an emergency action plan. This plan should be reviewed with local law enforcement before being finalized.
2. A map of the campgrounds and its immediate borders should exist so that all staff and local law enforcement are familiar with the camp, including areas they do not typically attend to (e.g. arts and crafts staff may not typically visit the sports field or archery range).
3. There should be camp protocols for deliveries, construction, repair work, etc.
4. Whoever is primarily responsible for security at camp should be known and identified easily by campers and staff, although markings indicating security should be strictly avoided.
5. The goal of conducting staff security-awareness training is to ensure that staff members understand expectations regarding security awareness and know they are responsible for being observant and reporting their observations to the designated camp staff member. Staff are not only encouraged to report unusual activity—they are required to do so. Training should enable staff to recognize suspicious activity and to take immediate action.
6. Staff training should address the following, at minimum:
   a. Review of the emergency management plan that includes:
      • Security protocols during normal activities—this includes what to look for that may be unusual or out of place (part of early detection). See #7 below for a list of such indicators.
      • Emergency management procedures
      • Evacuation and shelter-in-place strategies
      • Staff roles and responsibilities during normal activities, and when emergency occurs

The information provided in this document is designed to deliver helpful information on the subjects discussed. The information and references shared are the expert opinion of Paul DeMatteis, Global Security Risk Management, LLC, an independent consultant hired by JCC Association of North America. This document is not an alternative to local law enforcement protocols and advisement. The information within this document is meant for JCCs of North America and independent camps affiliated with JCC Association of North America. This document should not be copied, shared, or otherwise distributed outside the original intended recipients.

© JCC Association of North America, 2017
b. Working knowledge of all areas of the campgrounds

c. Security drills

d. In a given environment, what’s going on, what stands out and what will the staff person do?
   This applies to campgrounds and trips away.

7. Training should help staff look for anything that may be unusual or out of place. The following are examples of unusual activity:

a) Watchers
   1. Someone watching the campers at play; they might even look enthusiastic about the activity
   2. Someone watching and/or taking pictures of campers, buildings, front gate and other security controls and/or during evacuation drills, etc.
   3. Someone sitting in a wooded area watching the campgrounds (on or off your property)
   4. A drone flying over or near the camp
   5. Someone observing your camp from a road, hiking trail or neighboring property
   6. If water-accessible, someone monitoring your property or security protocols from a boat
   7. Someone asking for directions at the main gate or along the property line who does not appear to fit in

b. Strangers and Strange Behavior
   1. Someone you don’t know carrying bulky and/or heavy bags
   2. Someone you don’t know looking angry and/or annoyed
   3. While off-site, anyone showing unusual interest in your presence, inquiring about your camp or its security controls
   4. An individual hiking through your property
   5. Someone on your property asking for directions for a delivery or doing a repair
   6. An individual carrying equipment inconsistent with camping or hiking activities, military-type equipment, a GoPro, hunting gear during non-hunting season

c. Anomalies
   1. A locked door to a room in which hazardous chemicals (chlorine, gasoline, propane, etc.) are stored is found open
   2. Any indicators, including unauthorized campsites, that unauthorized persons might have been on your property
   3. Finding trail cameras on your property
   4. Suspicious calls, inquiries about security or emergency management or opinions on sensitive matters
   5. Something new in an area or in a building that could indicate a suspicious actor
   6. Something missing that might indicate an unauthorized person on your property
   7. Something moved to enable an individual to reach an upper window

The information provided in this document is designed to deliver helpful information on the subjects discussed. The information and references shared are the expert opinion of Paul DeMatteis, Global Security Risk Management, LLC, an independent consultant hired by JCC Association of North America. This document is not an alternative to local law enforcement protocols and advisement. The information within this document is meant for JCCs of North America and independent camps affiliated with JCC Association of North America. This document should not be copied, shared, or otherwise distributed outside the original intended recipients.

© JCC Association of North America, 2017
Any of these indicators could suggest a hostile act, but also could be harmless. However, individuals can analyze information uniquely and combine innocent observations into a suspicious pattern. All incidents must be evaluated and taken seriously; immediate evasive actions might be warranted until the situation has been clarified. For each observation, camps need to decide on and instruct and train staff in a preferred course of action. Regardless, all observations should be reported to a central person or office, and all observations should be recorded in detail.

8. All staff should have the following basic equipment and information (or access to it):
   a. A means or system of communication: walkie-talkies, cell phones and/or hand signals
   b. A flashlight and light sticks (for night activities)
   c. Small binoculars
   d. Extra batteries for all electronic devices
   e. Writing material
   f. Small air horn
   g. Trail-marking tape
   h. Camp map
   i. Updated list of emergency contact telephone numbers

9. Response to Threats
   Staff taking phone calls, checking email or monitoring social media should be trained in response to threats. The Department of Homeland Security and the FBI have resources for how to respond to threats, especially bomb and active shooter. Among them, staff should be familiar with and utilize the following:
   a. Guidance about bomb threats:
   b. Should you get a bomb threat:
      https://cdn.fedweb.org/137/268/DHS_Bomb_Threat_Checklist.pdf
   c. How to respond to an active shooter:
      https://www.dhs.gov/xlibrary/assets/active_shooter_poster.pdf

Further resources are available on the DHS and FBI websites, as well as dedicated sections of the Secure Communities Network (SCN) website https://scnus.org/resources/institutional-safety-and-securitylibrary/camps and the JCRC of New York website http://www.jcrcny.org/security-emergency

The information provided in this document is designed to deliver helpful information on the subjects discussed. The information and references shared are the expert opinion of Paul DeMatteis, Global Security Risk Management, LLC, an independent consultant hired by JCC Association of North America. This document is not an alternative to local law enforcement protocols and advisement. The information within this document is meant for JCCs of North America and independent camps affiliated with JCC Association of North America. This document should not be copied, shared, or otherwise distributed outside the original intended recipients.

© JCC Association of North America, 2017
Security Readiness

JUNE 2017: BULLETIN 04

EMERGENCY RESPONSE PLANS
AND
PROVIDING SAFE HAVENS
SECURITY BULLETIN 4

June 2017
EMERGENCY RESPONSE PLANS AND PROVIDING SAFE HAVENS

INTRODUCTION

This bulletin is the fourth in a series. Bulletin #1 introduced the four basic strategies for camps, as well as JCCs:
- Target hardening
- Early detection
- Appropriate response plans
- Providing safe haven

Bulletin #2 described more comprehensively the first two strategies of target hardening and early detection.

Bulletin #3 focused on Summer 2017 and what camps could consider for this summer, primarily in the area of building staff awareness around security.

Bulletin #4 addresses the last two strategies: emergency response plans and providing safe haven.

Emergency Response Plans includes sections on an Emergency Action Committee (EAC), response to bomb threats and warnings and considerations for when a bomb threat or warning is received.

Providing Safe Havens discusses in depth the five components of providing safe haven, and safe havens during a bomb threat event.

Strategy 3: Emergency Response Planning (ERP) for Security-Related Issues
The emergencies camps must confront can be categorized by the dimension of speed. Some, like hurricanes, are slow-moving events, allowing a comfortable margin of planning time. Others, like thunderstorms or tornadoes, move more quickly, allowing only a short warning period. Still others, like earthquakes, vehicular accidents and hostile acts, happen instantly, with no warning at all. This emergency response plan addresses this last category: suspicious activity, threats and acts of violence without warning. The next section provides a general overview and outline for your consideration.

The Emergency Action Committee (EAC)

Purpose
An Emergency Action Committee (EAC) is responsible for planning the response to critical events (suspicious person or package, bomb threat, act of violence, etc.). Having a response plan and training and drilling in its execution increases the likelihood of the best possible outcome. Once the emergency action plan is in place, the EAC continues to collect, analyze and maintain information gathered, brief members on local issues and update the plan as necessary.
Composition
The key camp decision-maker should chair the EAC. It should include members from the on-site senior management team and facilities or maintenance staff. Other off-site members could be a security director from your JCC (if applicable), management personnel and legal representation.

Each representative should have a deputy in case the primary is unavailable.

Operating Modes
The EAC has three operating modes:
1. Normal Mode, described above, in which the EAC convenes to review and revise the response plan.
2. Response Mode, in which the EAC convenes to analyze suspicious or threatening information and to discuss new threats and concerns (e.g., a bomb threat is received, and analysis is needed, and/or the bomb threat response plan must be implemented).
3. Implementation Mode, in which the EAC’s plan is put into immediate effect in response to a hostile act (e.g., an active shooter). In this mode, there is not time to convene an EAC meeting; the camp must rely on planning and training. It is critical that the head of the EAC, likely the off-site camp director, be empowered to work with local law enforcement and make emergency decisions.

Response to Bomb Threats and Warnings
Bomb threats are designed to hurt you or your organization. At the very least, they are meant to cause disruption and/or financial losses. The FBI and Department of Homeland Security (DHS) Office for Bombing Prevention have developed a Bomb Threat Guideline. It can be accessed here. DHS has also developed a Bomb Threat Phone Call Checklist for recording the caller’s information. In general, it relies on several key principles to group a threat into one of three categories: low risk, medium risk and high risk. Each of the threat levels considers how realistic the threat is, the knowledge of the caller, the target, event planning and explosives.

Below is real language or scenarios associated with different risk levels:

Low risk level might include:
- “I hope you all die in an explosion.”
- “There is a giant nuclear bomb in your building.”
- A threat presented by a caller known to you; he has called numerous times and his calls have been deemed non-life-threatening.

Medium risk level might include:
- “I have a bomb in my car, and I am driving to your location; I am going to kill you all.”
- “I have checked out your security, and I know how to get the bomb inside.”
- “I put the bomb in the kitchen, and it will go off in one hour.”
- “I put the bomb in the billiards room (no billiards room on-site) and I know how to build a pressure cooker bomb (vague information) and I really mean it.”

High risk level might include:
- “I’m coming to blow you up. I’ve tested my bomb and it will destroy the dining room and all of you.”
• "I used TATP this time, and it is better than the HMTD device I tested (actual explosive compounds)."
• "I want to get Howie and all his campers, and I know they are there; I’ve been watching. “
• "It’s going to happen today at dinner. After it happens, I want you all to know it was me, Ted."

Considerations for When a Bomb Threat or Warning is Received

• All bomb threats and or warnings must be taken seriously and analyzed. You should immediately initiate your search plan.
• A low-level threat might not need to be announced as long as a thorough search is conducted.
• Law enforcement should be notified of any threats. If possible, develop a working relationship with your local police department so that you can notify them discreetly. Too much local or media attention can increase your risk of more threats, possibly by different individuals.
• Many police departments will not be willing to assist you in analyzing the threat and might not use the FBI/DHS guideline. From a law-enforcement perspective, a threat is a threat, and not much difference is seen between the levels. They might tell you that you have to decide, or they might demand you evacuate.
• Numerous bomb threats occur on a daily basis in U.S. businesses and corporations. Threats are often handled internally by corporate security departments, and, in many cases, law enforcement is not even notified.
• However, should you actually find a bomb, law enforcement has the training and expertise to help you.
• If you must evacuate, make sure law enforcement is providing adequate protection for your campers when they are outside or exposed in a public area.

To Evacuate or Not to Evacuate

A bomb threat may also be used as a means to get people to move to an area where it is easier to cause harm. In general, more people can be hurt in the open and in public space than within your campgrounds. Moving campers during a bomb threat search or to a shelter-in-place location could place campers in an area where an active shooter or a bomber would have easy access to them. Therefore, do not automatically assume that evacuation is always the best course of action. Still, arrangements for transportation and a secondary location for shelter should be part of your emergency response plan in case there is ever a need to move campers and staff to an off-site location.

Warnings

The FBI/DHS guide does not address warnings. That may be because a warning is not a threat. Warnings might result from a third-party discovery of the plan:

“My husband hates all of you. He claimed you destroyed his life. He left the house in his pickup truck and said he’s going to kill you all.”

Or it might result from an individual active in the plot deciding he or she does not want to hurt innocent people.

If they are truly trying to stop the event, they are likely to give you the following information.
If they don’t, ask for it:
• Their name and contact information
• The name(s) and description(s) of the individual(s) involved in the plot
• If applicable, type of vehicle
• A cell phone number

The information provided in this document is designed to deliver helpful information on the subjects discussed. The information and references shared are the expert opinion of Paul DeMattei, Global Security Risk Management, LLC, an independent consultant hired by JCC Association of North America. This document is not an alternative to local law enforcement protocols and advisement. The information within this document is meant for JCCs of North America and independent camps affiliated with JCC Association of North America. This document should not be copied, shared, or otherwise distributed outside the original intended recipients.

© JCC Association of North America, 2017
The more information they give you, the more likely it is that the warning is real. Try to gather as much information as possible, but also let others nearby, including local law enforcement, know what is going on.

**Safe Havens as Part of Your Emergency Response Plan**
A safe haven is a location within the JCC to offer shelter while waiting for law enforcement to arrive and for other areas to be cleared. Safe havens are locations that:
1. Can be quickly and easily searched (boat house, dining hall, gymnasium, etc.)
2. Are freestanding, with sides and/or access points that can be easily searched (basement, roof, all interior space, and grounds around all exterior walls)
3. Are not adjacent or connected to buildings that are not searchable
4. Are not adjacent to any hazards (chemical or fuel storage). In larger camps, multiple buildings at opposite ends of the property may be required.

**Strategy 4: Providing Safe Havens**
This fourth strategy will focus on the concept of sheltering in place during an active shooter or hostile actor attack at your camp. In such an event, the level of training of leadership and staff translates directly into your ability to mitigate damage and loss. Staff must know what to do and take immediate action; there is no time for meetings or to give instructions. It is good to remember the following:

“We don’t rise to the level of our expectations; we fall to the level of our training.”

The three common protocols are to run, hide or fight. The particular dynamic of an event could change the order of these three responses.

**The Five Components of Providing Safe Haven**
This strategy addresses management, planning and training viewpoints covering the five issues below.
1. Concept and Strategy During an Active Shooter or Hostile Actor Attack
2. Sounding an Alarm and All-Clear Signal
3. Evacuation and Assembly Areas
4. Selecting Good Shelter-in-Place Locations for Your Camp
5. Making Structural Modifications (If Necessary) to Improve Forced Entry Resistance

**1. Concept and Strategy During an Active Shooter or Hostile Actor Attack**
Your staff will have the advantage of being in familiar surroundings, with location-specific planning and training. They should have a greater ability to help campers to safety.

Seconds count, and it is paramount to be prepared for an event of this type happening anywhere on your property, at any time, and to have the ability to quickly and appropriately respond. Questions that need to be addressed by your emergency response plan, or on the spot if not in the plan, include:
- Do we shelter in place, or escape the immediate area?
- Who calls local law enforcement?
- Where and when do we assemble after the all-clear has been sounded?
Preparatory Steps (Two Weeks Out to the Day Prior)

Develop/review emergency management plans with your staff, tenants and other organizations in the building or on the campus. This includes how you will communicate with participants should you need to make a quick decision to lock down or close the JCC. Check your calendar to familiarize yourself with what activities are taking place the day of the protest/rally, especially activities associated with groups that may be in the facility for the first time.

1. Know your exact property line so you are certain about when protesters infringe on your property. If your property is fenced and gated, be prepared to lock your gates if protesters are headed in your direction.

2. Begin to look for suspicious activity days before a plan to protest. This would include individuals studying your facility, suspicious visitors to the front desk, probing phone calls, etc.

3. If your facility is equipped with cameras, make sure they are operational, providing a clear picture and recording appropriately. If your facility is not equipped with security cameras, use smartphone cameras or personal video cameras to record disruptive activity. Do this covertly and only if safe.

4. Arrange for additional security for:
   a. The day before protests
   b. The day of the protests
   c. Possibly the day after protests

5. Depending on the size or impact of protest, law enforcement may be able to place a guard or guards at your facility. Off-duty guards would be your next-best option. Keep in mind that law enforcement may be very busy and unavailable. Your third option would be to hire the appropriate level of contract security guards. Explore options ahead of time; develop a plan involving one or more of these options prior to an event. Be prepared and plan ahead.

6. Be prepared to block your driveway or building approach with a heavy vehicle or truck.

7. Be prepared for the possibility of a cyber-attack. Be sure you will have all information and documentation you will need to function should your facility and/or systems be damaged and unavailable for several days.

8. On the day before the protest/rally/march, all cell phones and radios should be fully charged.
Preparing to Lock Down Your Facility
These are steps to be taken should your strategy be to lock down the facility, but not evacuate. Note that a lockdown is not the same as a shelter-in-place strategy; the latter necessarily involves the former, but you can have a lockdown without sheltering in place.

- Make sure you know who is involved with the decision to lock down the facility.
- In order to assure a quick lockdown of a facility and to confirm that all locking systems are functioning correctly beforehand, have staff run a thorough lockdown drill, practicing all procedures.
- In the event of a lockdown, should persons demand to leave, care must be taken to ensure that they are not let out of the facility directly into the conflict, and that the conflict is not let into the building as these people are let out.

Preparing to Close the Facility

- Be prepared to close down your facility the day of a protest. If conditions are unpredictable and there is a concern for your membership and staff, do not hesitate to close and make that announcement prior to the event. If a protest nearby is getting out of control once a facility has opened, be prepared to close and let staff and JCC participants out of harm’s way before an event escalates.
- Be sure you know who is involved with the decision to close the facility.
- Determine what the circumstances are and when the decision would be made to close the facility.
- Preplan a mechanism to notify all of your participants and staff if you have to close rapidly. It is recommended that all JCC participants and staff be made aware that the facility might be closed the day of a protest or closed during a protest. Make sure all are aware that information on the status of the facility can be obtained on your website, and persons should check the website before heading to the facility.
- Remember, closing may not be your first choice, but you do not want to put people (participants, children, staff, etc.) in harm’s way. If you have critical programs, try to move them to safe facilities.