Guidance and Considerations for Assessing & Improving Jewish Community Campus Safety & Security

Introduction

The purpose of this document is to provide information, guidelines, and recommendations to assist Jewish organizations and institutions located on community campuses with security planning. A key component of a successful safety and security strategy within the Jewish community involves establishing strong cooperation between organizations. A campus-wide, all-hazards approach that emphasizes the engagement of all tenant organizations and stresses the criticality of security awareness and training can have the greatest impact while also being the most cost-effective and sustainable. This document discusses questions to ask when developing a campus-wide security plan, common security concerns, vulnerabilities, and general recommendations to mitigate those vulnerabilities, along with security planning and implementation guidance.

Jewish Community Campuses

The very element that makes Jewish community campuses welcoming to the public is the factor that becomes the most significant threat. Jewish community campuses are typically open and welcoming to anyone and anything that crosses their boundaries. Jewish community campuses may contain educational, cultural, spiritual, wellness, and philanthropic programs in one location. They serve as a means of centralizing, elevating, and celebrating the services and resources of the Jewish community.

A Jewish community campus can be defined as two or more entities/facilities located on a common site that typically share some elements of the environment, such as parking, courtyards, vehicle access roads, or gates and entrances to connected or adjacent buildings. Typically, multiple addresses will be associated with the facilities, and in most cases, there is no single address for the campus as a whole. While individual campus entities may have the required 501(c)(3) designations allowing them to apply for physical security enhancements under the federal Nonprofit Security Grant Program (NSGP), many common areas, such as Jewish community campuses, fall outside the scope of the NSGP eligibility requirements, and entities are unable to secure NSGP funding for these vulnerable areas.

Facilities located on Jewish community campuses include Federation offices, Jewish Family Services, Jewish Community Centers, varying levels of Jewish educational programs and schools, and other community-based services and programs. When developing their physical security plans, these entities typically only focus on their respective facility without considering integration into an overall campus security plan. Protecting a Jewish community campus requires a multi-faceted approach to overall site security coupled with individual facility security. By leveraging advanced physical security technologies and strategically deploying security measures in layers, Jewish community campuses can create a comprehensive security strategy that ensures the security and safety of the tenant organization’s staff, visitors, students, and assets.

Proactive security planning and communication are essential to keeping a Jewish community campus safe during a critical incident. As the rate of antisemitism continues to grow, coordinated security and crisis management planning on Jewish community campuses becomes even more critical to the health and vitality of the community and those who use its services. A comprehensive campus-wide security plan will leave a campus better positioned to respond to and recover from a security breach. Developing a security plan involves educating all personnel and community stakeholders to recognize the need for a secure campus. Campus entities must work together to develop and implement a detailed and coordinated security plan.

Important questions to ask when developing a campus-wide security plan:

- How much involvement do entities have in the security procedures, processes, equipment, or personnel on the campus?
- Is there a primary entrance, and are the campus boundaries clearly defined? Establish a single point of entry to allow for vehicle and pedestrian access control.
- What is the current communications environment between entities? Share incident information across the organizations on campus for situational awareness — a standardized approach to incident management.
- Do individual entities and/or the campus employ professional guard services? Is there coordination between the various guard services? Are the guards armed?
- Has coordination with area first responders occurred to pre-plan for a campus-based response to an incident? Are there means to share security technologies with responding agencies?
- What security platforms does each entity have? Standardize security technology across campus — camera systems, alarm systems, access control, etc.
- Can the campus obtain a unique 501(c)(3) designation or unique address separate from tenant entities, thus permitting a campus-focused NSGP or other state grant application for physical security enhancements?

Common campus security concerns include the following:

- Lack of communication and security coordination between multiple separate and distinct entities.
- Varying access control, video surveillance, lighting, and emergency notification technology systems.
- Expansive areas with absent or limited area-wide security procedures and video monitoring.
- Campus-oriented security solutions that are beyond the scope of individual facility security measures.
- Open points of entry resulting from limited or no perimeter access control measures, including the lack of campus perimeter fencing.
- Poorly lit campus buildings, walkways, and parking areas with unkempt landscaping that obstruct visibility and provide places of concealment.
- Poorly communicated security and safety information for tenant entities and users.

Campus Vulnerabilities

Undefined Security Boundaries

Challenge — When security boundaries are undefined, it is difficult to determine who is responsible for responding to threats and/or emergencies at specific locations on the campus. Undefined security boundaries may confuse security personnel and visitors while disrupting the ability to deploy resources quickly and effectively. For example, an entity with a building positioned on a campus may view its outer perimeter as the building façade because it may believe the parking lot is the responsibility of the campus administration, while the campus administration may rely on the entity to be responsible for security matters related to the parking area.

Mitigation — Campus entities should work together and clearly communicate areas of responsibility to develop a campus-wide security plan that addresses potential threats and emergencies that affect the entire campus. Coordination of assets, campus-wide communications, and overlapping security functions should be established. An effective campus security plan consists of multiple consecutive layers of protective measures deployed in concentric circles around all entities, from the outer campus perimeter inward to the building and interior areas with the greatest need for protection. The layers are designed to detect, delay, and disable an attack as early as possible and at the greatest distance possible from each facility. Multiple layers reduce the risk of a single point of failure, which, if breached, may diminish the established security infrastructure. They also ensure that the security measures employed will be efficient when executed in the specified zone and segregated as needed, thus causing minimal operational interruptions.

Undesignated Campus Security Coordinator

Challenge — Typically, each entity will have a designated person responsible for security matters only related to their specific facility. However, most campuses do not have a campus-wide security coordinator to manage campus security needs across the multiple entities on the campus grounds. In addition, a campus security coordinator will work with local law enforcement agencies, municipalities, and security vendors for campus-wide security needs. Without a designated security coordinator, short- and long-term security-related matters may not be addressed, and organizational security-related interests may not be adequately achieved. A security vendor by itself cannot represent all the campus security-related matters as vendors are likely to see only a partial picture of an entity's functionality.

Mitigation — Assign a campus security coordinator to manage and regulate the security needs and interests of the entire campus and ensure collaboration and communication between all individuals responsible for individual entity physical security.

Campus-wide Security and Procedures Plan

Challenge — Individual entities may have internal written security procedures or plans that are specific to the entity and its respective facility. These plans typically are not shared across campus entities and do not account for campus-wide security issues.

Mitigation — A campus should have a written security plan and established procedures for the property coordinated between the tenant entities. Without a written plan, individual entities are less likely and, in some cases, unable to follow security procedures and protocols that affect other entities and the overall campus. The effectiveness of individual entity security operations will likely be degraded, exposing occupants to risks that can be addressed and mitigated in a comprehensive plan. Campus-wide procedures for handling emergency command and control responsibilities, incident reporting and investigations, lockdown plans, or suspicious device situations should exist to ensure all entities are aware of campus security incidents. Each entity should develop a written security and procedure plan that supports and is integrated into the campus-wide plan.

Campus-wide Mass Notification Plan

Challenge — The inability to send emergency alerts across campus is a vulnerability that can create panic, cause chaos, and even result in facility users finding themselves in harm's way. The effective dissemination of critical information to employees, stakeholders, facility users, parents, guardians, or students during a crisis is paramount to ensuring the safety and security of a campus environment.

Mitigation — Campus entities should work together to develop and establish a multi-layered mass notification plan for the overall campus. Users should be divided into each entity and then broken into related groups such as teachers, students, parents, security, parent-teacher association (PTA) members, staff, administration, and so on. A mass notification system, coupled with a locally audible public address system (PA), which can simultaneously send stakeholders automated notifications via landline, cell, text, email, social media, and/or mobile app, is advised, ensuring the message is received by all personnel, on- or off-site. Differentiation between routine mass notifications and emergency messages is highly recommended so as not to confuse recipients. Electronic messaging systems should be supported by audible and visual communications systems that can be activated quickly to transmit an alert tone, voice message, or visual alert (strobe) campus-wide during active emergencies.

Campus Assessments

These and other vulnerabilities are determined during a campus-focused Threat, Vulnerability, and Risk Assessment (TVRA). Discussed below are the main areas to consider when conducting a campus TVRA and developing a campus security plan. The TVRA should take a holistic view of the campus, with an understanding of the individual entity's functions and roles in the community, along with a detailed review of the existing physical security measures in place. In addition, a review of the campuses and each entity's physical security systems should be conducted. The specific physical security systems reviewed should, at a minimum, include the following:

Main Risk Considerations (TVRA)

- Video surveillance systems (VSS)
- Access control measures
- Intrusion detection systems (IDS)
- Emergency call boxes/phones
- Mass notification capability
- Facility lockdown capability
- Lighting
- Signage

Conducting an assessment and developing a campus security plan begins with the documentation and inventory of existing physical security measures, including any campus-wide measures and each entity's physical security measures. In addition to the tangible measures, there needs to be an understanding of each entity's security posture and security objectives. A campus-wide security plan must consider the impact it will have on each entity and its ability to achieve its scope and mission within the community.

Jewish community campuses should look towards the layered protection concept, which means placing a series of progressively more difficult obstacles in the path of an aggressor. These obstacles or physical security measures can be considered lines of defense. The first element of campus security design is to clearly define the boundary of the property. The campus boundaries serve as the first line of defense. Physical security measures here may be either natural, such as hostile vegetation, or manmade, such as a perimeter fence. In the absence of a physical barrier, the campus boundary should be clearly defined such that there is an evident separation from surrounding properties; this can be considered a psychological barrier. The psychological idea of barriers, such as property definition or territorial reinforcement, will not stop an aggressor. However, it can play an important role in defining a secure area.

Campus perimeter security directly affects the level of security necessary for the individual facilities within the campus boundaries. For example, a campus fence may preclude individual buildings from fencing their immediate perimeter. In addition, screening at the campus perimeter may assist with and enhance the screening of individuals as they enter individual facilities. A clearly defined outer boundary, along with signage, establishes an expectation of behavior and responsibility. A well-defined perimeter will discourage casual entrance onto the campus or into the campus buildings by people who might present a threat to campus facilities or occupants. The use of a campus-wide professional guard service posted at entry points and conducting routine patrols of the campus, can provide increased territorial reinforcement.

The second line of defense is controlling access to entities within the campus buildings. Access controls to campus facilities should be difficult to overcome. Access control is primarily considered door entrances, but facilities must also consider windows (a common point of break-ins) and opportunities for roof access. Electronic access control coupled with intrusion detection systems is an effective solution for securing a facility.

The third or final layer of defense includes individual facility interior control. This line of defense includes intrusion detection detection devices, mechanical and electronic access control, safe rooms, and asset protection measures. Video surveillance systems and access control measures span all three layers and should be deployed at each line of defense.

A coordinated campus security program benefits all entities by providing additional layers of protection. No one system, procedure, or policy can completely ensure the security and safety of a campus. Rather, it is the cumulative impact of proper security planning and implementation in the following four primary areas that yields the ideal outcome:

- **Have the appearance of and be a hard target.**
  - Present a strong security posture such that a potential perpetrator will not see the campus as an easy target and will turn away and look for an alternate target.
- **Utilize detection systems (cameras, guard services, alarms, alerts to staff and members, threat monitoring, etc.).**
  - Early detection will provide increased reaction time to a threat. Identifying a threat at the campus perimeter rather than at the entrance to the facility can result in lives saved.
- **Train and implement incident response plans and systems.**
  - Plan for, prepare for, and train for incidents. Implement campus-wide mass alert systems and ensure all tenants have access to emergency information. Routine training, drills, and exercises are paramount in campus security and safety.
- **Provide lockdown/safe room areas and emergency egress plans.**
  - Well-marked refuge areas and accessible emergency egress paths are essential. Preventing a threat from entering campus facilities is the goal, but plans must be in place to address a threat entry situation.

A campus culture that promotes security awareness — in which all entities identify and report suspicious persons, activities, and conditions — will greatly improve security for all.

The community should embrace the coordinated nature of a Jewish community campus and work together for the safety and security of entities. By working together, stakeholders on a Jewish campus can provide a safer and more secure environment for the Jewish community to thrive.

Reporting

Emergencies: 9-1-1

Security incidents:
Duty Desk: 844-SCN-DESK (844-726-3375)

Find your Security Professional

https://www.securecommunitynetwork.org/regions/

These guidelines are for informational purposes only. Secure Community Network (SCN) advises seeking professional security advice tailored to your situation. SCN makes no representation, guarantee, or warranty that adopting any recommendation presented here will ensure that your facility or users will be invulnerable to attack or crime. SCN shall not have any liability because of any decision by you to adopt or not adopt any part of these guidelines.

COMMIT TO ACTION