

OFFICE OF COMMUNITY SECURITY – SECURITY & VULNERABILITY ASSESSMENT

The Jewish Federation of Palm Beach County (JFPBC) Office of Community Security (OCS) Security & Vulnerability Assessment (SVA) is intended to increase the safety of your facility, its users, and visitors within a spectrum of practical limitations. The advisory recommendations in the SVA represent the best professional efforts and opinions of OCS based on its combined knowledge and experience.

JFPBC OCS does not represent that its assessment provides all options for improving or addressing security needs at your facility.

Organization Name:	
Physical Address of Organization:	

Section 1 – Assessor Information	
Assessment Conducted By: (Self-Assessment, Contracted Assessor, Local Law Enforcement, Fusion Center, Federal Agency, Associated Organization, Other)	
If 'Other' was selected, please list here:	
Name of each Assessor and any associated professional credentials: (Such as CPP, PSP, TLO, military, other security, inspection, or auditing credentials)	
Signature of the Assessor:	
Date of Assessment:	

Section 2 - General Information

Attach an aerial photo of the site that clearly shows the property line and all structures. <i>(Use an online mapping program to create an aerial photograph of the site.)</i>	
Unique Entity Identifier (UEI) Number:	
GPS Latitude & Longitude: <i>(Use an online mapping program to obtain coordinates for the site.)</i>	
Local Law Enforcement Agency: (Name & Address)	
Local Fire Department: (Name & Address)	

Section 3 – Background Information

(The data from this section should be used for general institutional background.)

Membership Size: (Include school populations.)	
Community Served: (Limit the information to the specific cities and counties served.)	
Outreach programs: (Youth, homeless, community, and missionary programs.)	
Onsite Facilities: (Include schools, libraries, event centers, cultural centers, medical centers, and worship centers.)	
Facility Use: (Does this facility allow unaffiliated groups to use facility, such as support groups, special needs programs, and is regular facility staff at the building during use.)	
Historical Artifact Preservation: (Historical artifacts present onsite that could be targeted.)	

Regional, National, or Historical Symbolism: (Limit the information to symbolism that relates directly to the site that could targeted.)	
---	--

Threat Assessment (TA):

Assessing threats is an important first step in security preparation. Coordination with the security assessor and local law enforcement can provide a clear picture of the current threats from terrorism, extremism, and criminal acts.

For the purpose of the TA, terrorism is defined as human-caused threats against persons or property to achieve political or social objectives. Extremism is defined as the holding of extreme political or religious views, fanaticism. Criminal Act is defined as an unlawful action or omission that violates a law forbidding or commanding it, which is punishable by the government.

Overall Description of Threat(s):	
List any <u>acts of terrorism, extremism or criminal activity</u> against persons or property directed at the site initiated to achieve political or social objectives during the last 5 years. Attach any photos, news articles or police reports that <u>validate the incidents</u>.	
Incidents	Describe the Impact on the site
1.	
2.	
3.	
4.	

(Add more lines as needed.)

Vulnerability Assessment (VA)

This VA assists assessors and institutions by collecting security related data on the organization and site. The VA can be used to track security improvements, adjust current security posture, and plan for future security needs.

The information should be collectively discussed so the organization can become more aware of the risks to the site and members. The document's intent is to assist in improving the entire security and safety posture of an institution and its members. The document can also be used to focus resources where needed the most.

Perimeter and Access Control Assessment	
Does the site, facility, or installations have a clearly defined perimeter? Is this perimeter boundary posted? (Yes or No/Describe if appropriate.)	
Does the site have perimeter fencing, and is this fencing maintained? Is the perimeter fence clear of vegetation and debris? Do you have a clear line of sight through the perimeter fence? (Yes or No/ Describe if appropriate or attach photos.)	
Are there known deficiencies in the security perimeter? Are deficiencies being corrected? What is the status? (Yes or No/ Describe if appropriate or attach photos.)	
Are Intrusion Detection System (IDS) sensors integrated into perimeter property line protection? (Yes or No/Describe if appropriate.)	
Does the organization effectively address all vehicle and pedestrian entry and exit points? Does the site, facility, or installation have high-speed avenues of approach? (Yes or No/Describe if appropriate.)	

Does the site, facility, or installations have illumination at any or potential security checkpoints to examine credentials, personnel, and vehicle? (Yes or No/Describe if appropriate.)	
Is the perimeter checked routinely by staff, volunteers, members, or security? (Yes or No/Describe if appropriate.)	

Security Lighting

Are doorways illuminated for security and safety? (Yes or No/Describe if appropriate.)	
Are pathways around the site illuminated to assist with movement and safety? (Yes or No/Describe if appropriate.)	
Is the lighting adequate to assist the security camera system to detect and identify activities around the site? (Yes or No/Describe if appropriate.)	
Are all identified critical areas covered by lights? Is the lighting adequate from a security perspective at roadway access and parking areas? (Yes or No/Describe if appropriate.)	
Does vegetation or debris obstruct illumination and or create dark shadows? (Yes or No/Describe if appropriate.)	

Security Intrusion Detection/Security Camera System/Fire System

Does the site, facility, or installations have a security center? Does the security center have adequate access control and alarm procedures? Is the security control center highly visible and has a secondary center been identified if the first one is affected by an incident? (Yes or No/Describe if appropriate.)	
Does the site have an operational intrusion detection system (IDS) installed on all windows, doors, skylights, crawl spaces, and roof hatches? (Yes or No/Describe if appropriate.)	
Does the intrusion detection system provide any specific or more focused coverage of identified critical assets? (Yes or No/Describe if appropriate.)	
Does the site have a security camera system in place? (Yes or No/Describe if appropriate.)	
Are all facility critical assets under security camera system coverage? (Yes or No/Describe if appropriate.)	
Are the security camera feeds and/or IDS systems monitored? (e.g., on-site, off-site, mobile) (Yes or No/Describe if appropriate.)	
Are security cameras and IDS sensors integrated to detect, identify, and respond to alarm activations? (Yes or No/Describe if appropriate.)	

Does the physical security protection system integrate the lights, cameras, fire alarms, and other sensors into a manageable security system? (Yes or No/Describe if appropriate.)	
Do the facility's systems directly communicate with local law enforcement and fire? (Yes or No/Describe if appropriate.)	

Security Operations

Does the facility use a security company, off-duty police, employees, volunteers, or members to perform security patrol operation? (Yes or No/Describe if appropriate.)	
Are entry control visual inspections evident at entry points? (Yes or No/Describe if appropriate.)	
Are after-hours checks made of the facility by security, employees, volunteers, or members? (Yes or No/Describe if appropriate.)	
Are the observations of the patrol documented in a daily security log? (Yes or No/Describe if appropriate.)	
Are there procedures for reporting suspicious personnel or activities? (Yes or No/Describe if appropriate.)	
Is there an effective employee entry control badge system, visitor pass system, or visitor escort policy and procedure? (Yes or No/Describe if appropriate.)	

How does the organization communicate with employees, volunteers, and members during emergencies? (Describe.)	
---	--

Vulnerability Assessment Attachment List (e.g., photographs, maps, diagrams)

Mitigation Options:

This section is designed to help identify vulnerabilities, consider potential consequences, and select target hardening (mitigation) options.

Mitigation options should be listed to address identified vulnerabilities or potential vulnerabilities. This section can be used to track requests for specific equipment, security needs, and prioritize target hardening projects.

List the vulnerabilities that could be exploited through acts of terrorism, extremism, or criminal activity directed at the site and organization. Also, provide a mitigation option for the vulnerabilities.
List the site's vulnerabilities, mitigation options, and potential consequences. <u>Mitigation Options</u> should describe the potential solution to the vulnerability.
Vulnerability:
Mitigation Option:
Vulnerability:
Mitigation Option:

Vulnerability:
Mitigation Option:
Vulnerability:
Mitigation Option:
Vulnerability:
Mitigation Option:
Vulnerability:
Mitigation Option:

(Add more lines as needed.)

Disclaimer

This document is provided by the Jewish Federation of Palm Beach County (JFPBC) Office of Community Security as an informational resource for you to consider in planning for your event. It is not an exhaustive list of security measures or best practices, and needs will vary by organization, facility, and threat environment. JFPBC, its staff, lay leadership, and affiliates make no representation that implementing any guidance herein will prevent or mitigate any security incident, threat, injury, loss, or damage. Each organization is solely responsible for consulting qualified legal, security, and insurance professionals before implementing any security program or practice.

This document reflects information available at the time of publication and is subject to change without notice. Users are responsible for verifying that, at the time of use, this guidance is current, accurate, and applicable to their specific circumstances.

By providing this information, JFPBC is not undertaking any obligation or responsibility for the security of your event or organization. Your organization and its leadership are solely responsible for determining what procedures it implements and the performance of those procedures by your employees, vendors, agents or volunteers.