Security Program

Self-Assessment Checklist

For Jewish Organizations

Jewish Federation of Palm Beach County • Office of Community Security

Revised: 6/3/2026

Organization / Facility Name:	**Date of Assessment:**
Completed By:	**Title / Role:**

How to Use This Checklist

The self-assessment is intended to provide a framework to enhance security. While it is understood that each organization's situation, resources, and preparedness vary, this checklist offers security best practices and guidance to improve your organization's overall security posture. Check the box next to each item your organization has implemented. Items left unchecked represent areas for security improvement. Use the assessment to note items in progress and/or rank potential security projects by need. Review with executive leadership and revisit at least annually after any significant security incident or improvement is made. Note that the checklist mirrors guidance listed in Comprehensive Security Program Best Practices.

1. Program Foundations & Available Resources

Assessment checklist

□	Budget and long-term sustainability assessed
□	Funding sources identified (federal, state, philanthropic)
□	Existing infrastructure and facility layout evaluated
□	Scope of program coverage determined (single site vs. multi-campus)

☐	In-house expertise vs. outside consultants assessed
☐	Available professional guidance and assistance identified
☐	Partner organizations established

Jewish security partnerships (professional relationships, information resources, training opportunities, website links for reporting purposes, etc.)

☐	Federation Office of Community Security (OCS)
☐	Secure Community Network (SCN)
☐	Community Security Initiative (NY)
☐	Community Security Service (CSS)
☐	Anti-Defamation League (ADL)

2. Threat & Vulnerability Assessments

Assessment topics addressed

☐	Physical vulnerabilities
☐	Technical vulnerabilities
☐	Personnel risks
☐	Social media threat monitoring
☐	Cybersecurity
☐	Area crime statistics
☐	Federal, state, and local threat environment
☐	Assessments related to key staff and stakeholders (if necessary)

Process completed

☐	Findings formally documented
☐	Reviewed with executive leadership and key stakeholders
☐	Bi-annual review schedule established (or after significant incidents)

☐	Lessons learned incorporated from any prior security activations

3. Physical Security (Facility Target Hardening)

Structural hardening

☐	Windows addressed (film, reinforcement as needed)
☐	Doors upgraded (solid core, reinforced frames and hardware)
☐	Door locks reviewed for compliance with fire codes and regulations
☐	Fenceline and gates assessed
☐	Perimeter access control in place
☐	Entry screening procedures established
☐	Vehicle access control measures implemented
☐	Lighting and landscaping improvements completed

Entry management

☐	Controlled single-point entry during programming
☐	Doors locked to prevent exterior access during school or service hours
☐	Visitor sign-in with identification procedures established
☐	Staff and volunteer badging system implemented

4. Technical Security Plan

Surveillance systems

☐	Interior and exterior camera systems installed
☐	Live monitoring during high-risk events arranged
☐	Video retention protocols established

Access control & identification

☐	Electronic keycard systems installed

□	Controlled door access implemented
□	Lock upgrades completed
□	Inspection systems in place
□	Personal access control credentials issued

Communication systems

□	Two-way radios distributed to staff and security
□	Emergency mass notification system in place
□	PA system integration completed
□	Redundant communication devices available for large events

5. Personnel Security Plan

Guarding strategy

□	Armed vs. unarmed guard decision made and documented
□	Private security vs. off-duty police decision made
□	Clear post orders and standard operating procedures (SOPs) documented
□	Defined chain of command established
□	Required insurance coverage confirmed for all security personnel
□	Ongoing training requirements established for security staff

If using private security companies

□	References checked
□	Interviews conducted
□	Licensing and liability coverage confirmed
□	Trial period requested

6. Safety & Security Training

Training completed

□	Stop the Bleed
□	First Aid
□	AED training (hands-on use)
□	Situational awareness
□	De-escalation techniques
□	Run, Hide, Fight protocol
□	Additional training to address specific needs or requirements

Readiness confirmed

□	Staff know locations of AEDs, first aid kits, and Stop the Bleed kits
□	Training reflects needs of elderly members, children, individuals with disabilities, and those with physical restrictions
□	Annual drills conducted (lockdown, evacuation, fire, severe weather, etc.)

7. Insurance & Risk Management

Coverage reviewed

□	General liability (no firearm exclusion; $1M occurrence / $2M aggregate minimum)
□	Workers' Compensation ($1M bodily injury by accident, disease policy limit, disease per employee)
□	Professional liability ($1M minimum)
□	Commercial auto, if applicable ($1M minimum)
□	Umbrella ($5M minimum, no firearm exclusion)
□	Facility-specific liability
□	Armed guard liability coverage (no firearm exclusion)
□	Event-specific insurance arranged as needed

Process completed

□	Annual insurance review scheduled with faith-based/nonprofit-familiar broker
□	Local, state, and federal legal requirements reflected in coverage
□	Institutional self-coverage
□	Guard company coverage via contracted services

8. Law Enforcement & Intelligence Coordination

Outreach completed

□	Local police departments (jurisdiction-specific)
□	County sheriff's office
□	State police
□	Federal law enforcement
□	Local, state, and national intelligence centers

Best practices in place

□	Facility walkthroughs completed with law enforcement
□	Tabletop exercises completed with law enforcement
□	Participating in law enforcement threat briefings
□	Event calendars shared with law enforcement when appropriate
□	Registered with local intelligence/fusion centers

9. Emergency Services Coordination

Relationships established

□	Fire department
□	EMS providers

Coordination completed

☐	Facility walkthroughs completed with fire/EMS
☐	Emergency access routes identified and shared
☐	Staging areas designated
☐	AED and medical kit locations shared with emergency services

10. Emergency Planning & Crisis Management

Plans documented

☐	Emergency communication plan
☐	Community and organizational communication/notification plan
☐	Crisis management plan
☐	Evacuation plans
☐	Severe weather plans
☐	Shelter-in-place procedures
☐	Reunification protocols (if youth programming is present)
☐	Tabletop exercises conducted

After any activation

☐	Formal After-Action Report (AAR) completed
☐	Improvements and lessons learned documented

11. Location-Specific & Community Considerations

Evaluated in consultation with key stakeholders

☐	Federal, state, and local laws reviewed for security implications
☐	Local crime statistics reviewed
☐	Shared campuses or partner organizations assessed

☐	Parking and traffic flow vulnerabilities evaluated
☐	Protest risks evaluated
☐	Mental health considerations addressed in security planning
☐	Physical restrictions and disability accommodations addressed
☐	Age-specific safety concerns addressed

12. Additional & Miscellaneous Considerations

Additional items

☐	Internal reporting mechanism for suspicious activity established
☐	Social media monitoring during sensitive events in place
☐	Volunteer coordination policies documented
☐	Documentation retention protocols established
☐	Periodic program audits scheduled
☐	Annual board-level security review scheduled
☐	Grant application strategy for security funding developed

13. Notes

Disclaimer: *This document is provided by the Jewish Federation of Palm Beach County (JFPBC) Office of Community Security as an informational resource. 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. Revised: 5/19/2026.*