

Comprehensive Security Program

Best Practices

For Jewish Organizations

Jewish Federation of Palm Beach County • Office of Community Security

Revised: 6/3/2026

In the current environment, particularly post–October 7, security must be structured, resourced, intelligence-informed, and continuously evaluated. A true security program is not just guards and cameras — it is governance, planning, partnerships, training, insurance, compliance, and community culture.

1. Program Foundations & Available Resources

Before implementation or expansion, leadership should assess:

Available Resources

- Budget and long-term sustainability
- Funding sources (federal, state, philanthropic)
- Existing infrastructure and facility layout
- Scope of program coverage (single site vs. multi-campus)
- In-house expertise vs. outside consultants
- Available professional guidance and assistance
- Partner organizations

National Jewish Security Partners for guidance and intelligence coordination may include:

- Secure Community Network
- Community Security Service
- Community Security Initiative – NY
- Anti-Defamation League

Security planning must align risk level with operational capacity and financial reality.

2. Threat & Vulnerability Assessments

Conduct formal threat-vulnerability assessments of all facilities and keep documentation current.

Assessment Should Include:

- Physical vulnerabilities
- Technical vulnerabilities
- Personnel risks
- Social media threat monitoring
- Cybersecurity
- Area crime statistics
- Federal, state, and local threat environment
- If necessary, assessments related to key staff and stakeholders

Process

- Document findings formally.
- Review with executive leadership and key stakeholders.
- Update bi-annually or after significant incidents.
- Incorporate lessons learned from any security activation.

This assessment becomes the foundation of the security program.

3. Physical Security (Facility Target Hardening)

Develop and implement a **Facility Target Hardening Plan** tailored to each location.

Structural Hardening

- Windows (film, reinforcement as needed)
- Doors (solid core, reinforced frames, and hardware)
- Door locks with special attention to specific fire codes and other regulations
- Fenceline and gates
- Perimeter access control
- Entry screening procedures

- Vehicle access control measures, including the potential addition of physical structures
- Lighting and landscaping improvements

Entry Management

- Controlled single-point entry during programming
- Lock doors preventing exterior access during school or service hours
- Visitor sign-in with identification procedures
- Staff and volunteer badging system

Physical security must reflect local laws and crime patterns.

4. Technical Security Plan

Develop and implement a written **Technical Security Plan** including:

Surveillance Systems

- Interior and exterior camera systems
- Live monitoring during high-risk events
- Video retention protocols

Access Control & Identification

- Electronic keycard systems
- Controlled door access
- Lock upgrades
- Inspection systems
- Personal access control credentials

Communication Systems

- Two-way radios for staff and security
- Emergency mass notification systems
- PA system integration
- Redundant communication devices during large events

5. Personnel Security Plan

Develop and implement a formal **Personnel Security Plan** addressing:

Guarding Strategy

- Armed vs. unarmed guards
- Private security vs. off-duty police
- Clear post orders and Standard Operating Procedures (SOPs)
- Defined chain of command
- Required insurance coverage
- Ongoing training requirements

If using private security companies:

- Check references
- Conduct interviews
- Confirm licensing and liability coverage
- Request a trial period

6. Safety & Security Training

Arrange diverse types of training to build a culture of preparedness.

Recommended Training

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

Ensure:

- Staff know locations of AEDs, first aid kits, and Stop the Bleed kits.
- Training reflects the needs of elderly members, children, individuals with disabilities, and those with physical restrictions.

- Drills are conducted annually (lockdown, evacuation, fire, severe weather, etc.).

7. Insurance & Risk Management

Identify and review appropriate insurance coverage annually. Examples of minimum insurance coverage amounts are noted for consideration.

Coverage Considerations

- General liability with no firearm exclusion
 - \$1 Million Occurrence / \$2 Million Aggregate
- Workers' Compensation
 - \$1 Million – Bodily injury by accident (each accident)
 - \$1 Million – Bodily injury by disease (policy limit)
 - \$1 Million – Bodily injury by disease (each employee)
- Professional Liability
 - \$1 Million Minimum
- Commercial Auto (if applicable)
 - \$1 Million Minimum
- Umbrella
 - \$5 Million minimum with no firearm exclusion
- Facility-specific liability
- Armed guard liability coverage (no firearm exclusion)
- Event-specific insurance

Insurance review should be coordinated with brokers familiar with faith-based and nonprofit institutions. In addition, consideration should be given reflecting local, state, and federal legal requirements.

8. Law Enforcement & Intelligence Coordination

Conduct proactive outreach with:

- Local police departments (jurisdiction-specific)
- County sheriff's office
- State police
- Federal law enforcement

- Local, state, and national intelligence centers

Best Practices

- Facility walkthroughs
- Tabletop exercises
- Participation in law enforcement threat briefings
- Sharing event calendars when appropriate
- Registering with local intelligence/fusion centers

Ongoing coordination builds both deterrence and rapid response capability.

9. Emergency Services Coordination

Establish relationships with:

- Fire departments
- EMS providers

Include:

- Facility walkthroughs
- Emergency access routes
- Staging areas
- AED and medical kit locations

10. Emergency Planning & Crisis Management

Develop and maintain documented emergency plans:

Required Plans

- Emergency communication plan
- Community and organizational communication/notification plans
- Crisis management plan
- Evacuation plans
- Severe weather plans
- Shelter-in-place procedures

- Reunification protocols (if youth programming is present)
- Tabletop exercises

If a plan is activated:

- Conduct a formal After-Action Report (AAR)
- Document improvements and lessons learned

11. Location-Specific & Community Considerations

After consultation with key stakeholders, evaluate:

- Federal, state, and local laws
- Local crime statistics
- Shared campuses or partner organizations
- Parking and traffic flow vulnerabilities
- Protest risks
- Community-specific needs:
 - Mental health considerations
 - Physical restrictions and disabilities
 - Age-specific safety concerns

Security must reflect the unique character and vulnerabilities of each facility and community.

12. Additional / Miscellaneous Considerations

- Clear internal reporting mechanism for suspicious activity
- Social media monitoring during sensitive events
- Volunteer coordination policies
- Documentation retention protocols
- Periodic program audits
- Annual board-level security review
- Grant application strategy for security funding

Strategic Framing for Leadership

Security is no longer an operational afterthought. It is core infrastructure and a fiduciary responsibility.

While the need for a comprehensive security program is common to all Jewish organizations, there is no security “one size fits all” solution. Each program must be tailored to a specific location reflecting realistic goals based on threat level, support, adaptability, and available resources. Each program should also strive to integrate technical, physical, and personnel security to strengthen the overall security posture.

The modern Jewish organization must shift:

From *informal safety practices* → **to structured security programs.**

From *reactive incident response* → **to ongoing risk management.**

From *isolated decision-making* → **to coordinated intelligence-driven planning.**

The goal is not to create a fortress.

The goal is to create a resilient, prepared, and confident community.

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.