Direct from an ASIS INTERNATIONAL COUNCIL

White Paper Cultural Properties Council - House of Worship Sub-Committee

PREPARING A SECURITY RESPONSE PLAN FOR HOUSES OF WORSHIP

White Paper

November 2020

ASIS Houses of Worship Sub-Committee.

Contributions by Nathan Bearman (Editor), Jim McGuffey (House of Worship Chair), Paula Ratliff Pedigo, Robert A. Wilson, Andy Davis (Cultural Council Chair), David Bacall, Paul Myers, Paul Huston, John Griffey, Phil Purpura, Carl Chinn, James Reaves, and others.

Introduction & Foreword

Houses of worship (HOW) are meant to be sanctuaries of peace and tranquility in an otherwise chaotic world. Throughout history, however, they have unfortunately faced challenges including terrorism, racism, hatred, xenophobia, Islamophobia, anti-Semitism, looting, and vandalism but to name a few.

Houses of worship would typically include **Churches, Temples, Mosques, Synagogues, Shrines, Monasteries** & other sites considered holy or sacred to religious orders. They could be as large as the Notre Dame cathedral or as small as an intimate prayer room in somebody's home.

This document has been prepared by security professionals as a tool to assist individuals that belong to these houses of worship in preparing a security & emergency management plan.

The goal of this planning is to **help mitigate these risks** and prepare these facilities in the event they are targeted. A formal structured plan will also help educate the community so that a coordinated effort and response can be in place.

This document is aimed at all sizes of faith communities from those numbering only a few dedicated individuals up to modern mega communities with hundreds or even thousands of members and whilst some of the more robust security measures that are outlined may not be appropriate for all, they are applicable for those where risk levels warrant their application.

Hopefully, there are parts of this paper that can be used by many faith-based organisations to help them add relevant security countermeasures that help improve safety and security at places of worship.

As security professionals, the **prevention of loss of life is paramount** in the planning and protection of the faith community's way of life.

In addition to the place of worship, care should be taken to protect associated sites where worshipers gather, including cemeteries, youth camps, pilgrimage sites, religious shops, and religious schools.

No guide can cover all situations and risks, but we hope this guide will serve as a solid foundation in your organization's planning and mitigation. It should be accompanied where possible with advice and guidance from security professionals and national or local law enforcement.

It is most important that your plan be your plan and specific to your site, faith, demographics, and local laws or policies.

Please note that different countries, states, provinces, and counties may have different laws relating to private security, security volunteers, & of course firearm use.

It is always important to follow the laws of your country and never do anything illegal in terms of protecting your house of worship.

Please feel free to build on this plan and adapt it to suit your HOW facility and community.

Nathan Bearman (Editor)

Plan Structure & Purpose

Structure

A security and emergency plan should begin with a cover page, followed by a table of contents, and a log of document revisions. The log should specify the dates of when revisions were made, a summary of the revision, and signature(s) of leadership indicating their approval of the plan.

Purpose

- All organizations should have appropriate security and/or emergency plans in place to deal with the potential and actual threats facing that organization. This is a sound business practice recognized by **ASIS International**.
- Any plan should be aligned to the organization's operations, goals, and founding principles.
- The objective is to communicate a clear message about the plan and the climate in which it was written.
- This section should serve as a directive to the planning team. It should set the parameters and explain why the planning is necessary, including what you hope to accomplish by creating the plan. As an example:

'The purpose of this plan is to set policies and programs in place to protect our house of worship, facilitate a fast and effective response to emergencies, and provide services that protect our worshipers should a crisis arise.'

Plan Maintenance

- Set instructions for how often the plan will be reviewed and revised (as needed) and by whom, e.g., at least annually, after emergency exercises, and actual emergencies.

Authorities and References

- Ensure the HOW makes appropriate use of security industry best practices such as the ASIS International Protection of Assets (POAs) resources.
- Ensure the HOW consults with the appropriate local, federal, national, or the required government bodies concerning the plan.
- Ensure all planning and measures are in line with local laws, regulations, and guidelines.
- Consult with security & emergency planning professionals.

Organization

- Outline the organizational structure of your HOW, including leadership, staff, communication officer, and the security team.

Concept of Operations

- Provides a broad overview of how the HOW addresses emergencies, including responsibilities of the HOW before, during, and after an emergency or disaster and the HOW security team and communication officer who will support the site in an emergency.

TABLE OF CONTENTS

Section 1: HOW Site Information & Layout

An important starting point for an emergency security plan is the documentation relating to the site's existing information, including appropriate contact details, responsible individuals, and site/equipment layouts.

Site Name:	Facility name (official or unofficial)	
Operating Hours:	Hours of services, regularly scheduled events, delivery times.	
Geographical Location:	The physical address and closest intersections. If your access point is at a different address, or you have multiple access points, you should include those here, too.	
Safety Information:	Important information about your site that may determine how the site will respond in an emergency or how emergency responders would respond to your site, e.g., construction material, staff numbers), other groups or organizations that use the site, etc.	
Emergency Contact **Details:**	★ **Responsible Police Station**	
	★ **Law Enforcement Liaison Officer**	
	★ **Bomb Squad**	
	★ **Closest Army Base**	
	★ **Fire Department**	
	★ **Emergency Medical Service (Private and/or State)**	
	★ **Closest Hospital**	
	★ **Security Companies**	
	★ **Emergency Plumber**	
	★ **Emergency Electrician**	
	★ **Electronic Security Service Tech**	
	★ **Undertaker/Burial Society**	
	★ **Landlord**	
	★ **Pest Control**	
	★ **Municipal Gas**	
	★ **Municipal Water**	

	★ **Municipal Electricity**	
	★ **Municipal Refuse**	
	★ **Other**	
After Hours Contacts:	★ HOW Facility Keyholder(s) ★ Caretaker ★ HOW Security Team (if one exists) ★ Clergy ★ Senior Staff ★ HOW Communication Officer, Board Members, & Custodians	

Layout Drawings (Structure, Entry/Exit Points, & Security Measures)

These drawings will assist the HOW team and/or law enforcement in terms of security planning, operational security work, and in the event of an emergency such as an evacuation, active attacker, and/or hostage drama. Base plans can be acquired from the facility architect, the local council, or one can use Google Earth as a good basis for the overall layout of the site. The following should be included:

Structural & Other

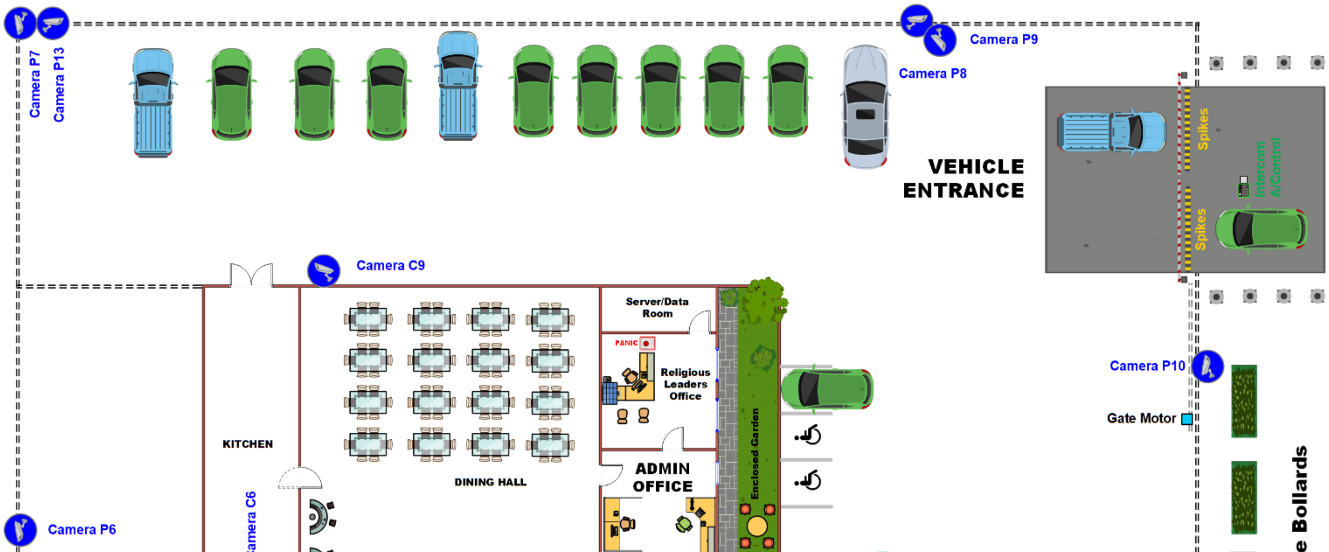
- Perimeter type (fence, wall, brick, welded mesh, palisade, etc.).
- Walls, window, doors, barriers, and gates.
- Natural boundaries such as water, foliage, or extreme landscape changes (cliff, mountain, etc.).
- Gas, water, or electrical power shut-off points.

Security Measures

- Sensors, video surveillance, intrusion detection, perimeter detection, panic buttons.
- Gate automation, vehicle barriers, vehicle bollards.
- Security officer postings, guard rooms, and/or control rooms.

Emergency

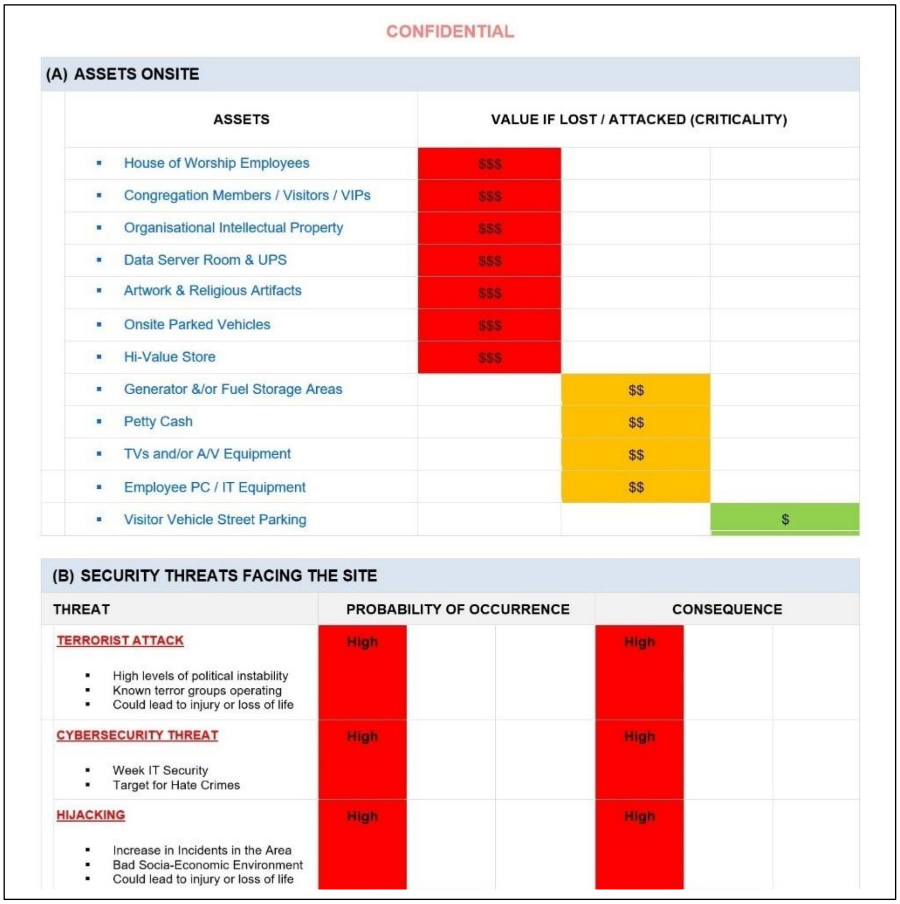
- AEDs, medical oxygen, first aid rooms, & medical bags.



Section 2: Security & Risk Survey

A security and risk survey is an essential tool for **identifying vulnerabilities** at a site. An initial survey should be conducted as part of this plan and regular audits carried out post issuing the plan.

- A good approach is to ensure **critical assets are identified and prioritized** for protection; **threats and hazards are identified** and evaluated to determine the **probability of occurrence** and the **possible consequences** (criticality), and cost-effective security countermeasures are assigned to mitigate risk and enhance recovery.



CONFIDENTIAL

(A) ASSETS ONSITE

ASSETS	VALUE IF LOST / ATTACKED (CRITICALITY)		
House of Worship Employees	$$$		
Congregation Members / Visitors / VIPs	$$$		
Organisational Intellectual Property	$$$		
Data Server Room & UPS	$$$		
Artwork & Religious Artifacts	$$$		
Onsite Parked Vehicles	$$$		
Hi-Value Store	$$$		
Generator &/or Fuel Storage Areas		$$	
Petty Cash		$$	
TVs and/or A/V Equipment		$$	
Employee PC / IT Equipment		$$	
Visitor Vehicle Street Parking			$

(B) SECURITY THREATS FACING THE SITE

THREAT	PROBABILITY OF OCCURRENCE			CONSEQUENCE		
TERRORIST ATTACK ▪ High levels of political instability ▪ Known terror groups operating ▪ Could lead to injury or loss of life	High			High		
CYBERSECURITY THREAT ▪ Week IT Security ▪ Target for Hate Crimes	High			High		
HIJACKING ▪ Increase in Incidents in the Area ▪ Bad Socia-Economic Environment ▪ Could lead to injury or loss of life	High			High		

- Part of the security risk assessment is to verify that an emergency management and continuity plan exists and is practised with the appropriate agencies within your community and evaluated for weaknesses on an as-needed basis. If it doesn't, one needs to be created.
- External review and discussion can put another set of eyes on your facilities such as local law enforcement and public safety officials to obtain their professional opinions.
- An **outside-inside** approach to the survey will look at the measures an adversary needs to overcome to target the asset which is the HOW. Think about how you would attack the facility.
- An **inside-outside** approach will highlight the view from the facility's defenders.
- A **security audit** is generally a follow-up security survey where the site is checked against a previous report, a checklist, or against the security plan itself.

Assets, Threats, & Vulnerabilities

(A) Assets (Measured in terms of priority such as loss of life and replacement cost)

- Congregants, Employees, & Volunteers
- Religious & Historical Artifacts
- Cash (Donations, etc.)
- Community Database (Donor Info, etc.)
- Intellectual Property & IT Equipment
- Kitchens, Perishable Goods, + Goods Store
- Visitor, Employee Property (Vehicles, etc.)

Religious Artifacts

(T) Threats (Adversarial)

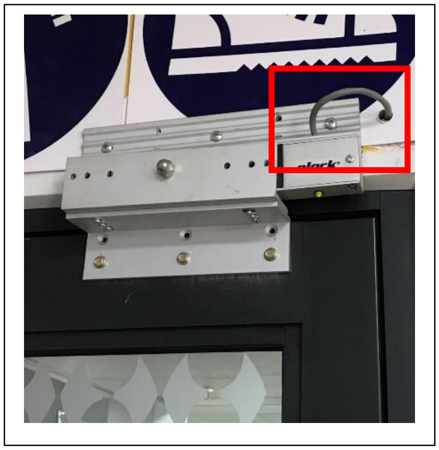
THREAT		THREAT	
Arson		*Mail/Parcel Bomb*	
Active Shooter		*Medical Emergency*	
Agent Provocateur		*Muggings*	
Car Bomb		*Petrol Bombing*	
Cyber Attack		*Protest March*	
Bio/Chem/Nuclear Attack		*Riot/Pogrom*	
Building Collapse		*Saboteurs*	
Burglary		*Sexual Attack or Abuse*	
Desecration		*Stabbing Attack*	
Drive-By-Shooting		*Suicide Bomber*	
Fire		*Vandalism/Looting*	
Flooding		*Vehicle Rammer*	
Hostage Taking		*Other*	

(T) Threats (Natural)

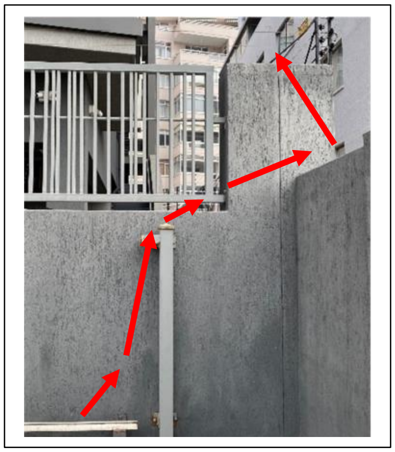
THREAT		THREAT	
Cyclone/Tornado		*Mudslide/Avalanche*	
Drought		*Pandemic*	
Earthquake		*Tsunami*	
Flooding		*Lightning*	
Heatwave Cold Wave		*Heavy Snow/Ice*	
Wild Animals		*Other*	

(V) Vulnerabilities (Every site will be different; below are some examples)

VULNERABILITIES			
Access Control Vulnerable to Tampering		*Poor Management or Loss of Access Control Credentials*	
Access Control Doors Left or Propped Open		*Video Recorder Susceptible to Theft*	
Video Recorder or Cameras Offline		*Electric Fencing Not Operational*	
Alarm System Faulty		*Overgrown Foliage*	
Poor Perimeter or Parking Lot Lighting		*Easy Accessibility to Highways/Roads*	
Insider Staff Threats		*Non-Working Intercom*	
Insufficient Video Recording Storage		*Perception of Poor Security @ the Site*	
Security System Single Point of Failure		*Damaged, Broken, or Cut Fencing*	
Poor IT Security		*Unprotected Windows*	
Lack of Security System Maintenance		*Easily Scalable Perimeter Fence/Wall*	
Power Failures		*Other*	



Unsafe Side Lock Wiring

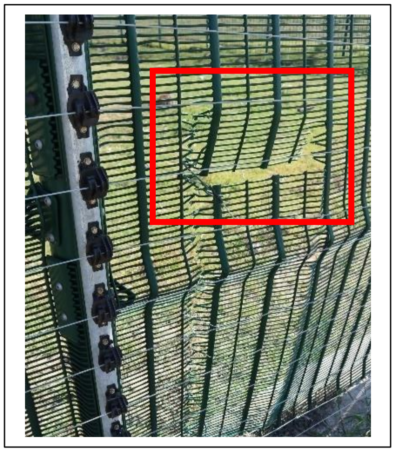


Vulnerable Perimeter

Lost Tags/Cards Not Removed

A/C Door Propped Open

Recorder can easily be stolen



Damaged Fencing

® **Risks**

RISK		RISK	
Ageing Community & Emigration		*Neighbouring & Peripheral Properties*	
First Responder Response Times		*Organized Crime or Gang Violence*	
Homelessness		*Political Environment*	
Deteriorating Healthcare Facilities		*Socio-Economic Climate*	
Local Crime Rate		*War or Civil Unrest*	
Local IT Infrastructure		*Pandemic*	

Existing Security Measure Checklist

As part of the security survey, the existing security mitigation measures in place at the HOW facility would need to be evaluated & notes recorded of the status of these at the site. They would include a combination of the following:

(A) Manpower

	Yes / No	*Status*	*Comments*
Security responsible individual			
HOW security volunteers			
Staff Trained in First Aid			
Staff Trained in Fire Fighting			
Security Officers			
Private or HOW employed			
Armed or unarmed			
Uniformed or Plain Clothes			
HOW Internal Response Team			
Law Enforcement			
Panic buttons (armed/unarmed response)			
Security Equipment (search mirrors, torches, non-lethal weapons, etc.)			
Security Guard Tour System			
Offsite CCTV Monitoring			
Guard dogs			

(B) Physical Building

	Yes / No	*Status*	*Comments/Type*
Perimeter - Welded mesh fence			
Perimeter - Palisade fence			
Perimeter - Wire mesh fence			
Perimeter - Brick wall			
Perimeter - Concrete block wall			
Perimeter - Electric fence			
Perimeter – Natural, i.e., Water, Foliage, Cliff, etc.			
Vehicle Perimeter Barriers			
Security Gatehouse			
Main - Entrance gate			
Main - Entrance door			
Door - High Security			
Door - Locks standard			
Door - Locks high security			
Door - Barricade devices			
Window - Burglar bars			
Window - Glass laminate			
Windows - Bulletproof			
Window - Protective mesh			
Operational Fire escapes			
Staff Locker Area			
Safes for Storage of cash/valuables			
Safe Room/Refuge Area/ Shelter-In Place/Panic Room			

(C) Technical

Technical security measures normally include sensors, visual aids, automation, or other items to aid in the detection of security anomalies and communication in the event of an emergency.

	Yes / No	*Status*	*Comments/Type*
Biometric Access Control			
RFID Access Control			
Mechanical Access Control			
Vehicle Access Control			
Intercom System (External)			
Intercom System (Internal)			
2-Way Radios			

Cellular Communication			
Fence Detection System			
External Intrusion Alarm			
Internal Intrusion Alarm			
Alarm Panic Buttons			
Fire Escape Door Monitoring			
Door Prop Alarms			
Alarm Siren/Strobe			
Burglary Counter Measures Such as Fog or Noise			
Alarm Radio Transmitter			
Fire Detection System			
Fire Extinguishers			
Stretchers/Evacuation Tools			
Medical Kits/First Aid Kits			
Gate Automation			
Vehicle Barriers			
Lighting (Perimeter)			
Lighting (Parking)			
Lighting (Internal)			
Video Surveillance (Perimeter)			
Video Surveillance (Internal)			
Video Recording System			
Remote Video Monitoring			
Electronic Visitor System			
Battery Backup System			
Generator Backup System			
Baggage XRAY			
Walk-Through Metal Detector			
Man-Trap Access Control			

(D) Information Technology

	Yes / No	*Status*	*Comments/Type*
IT Security Policy			
Security Firewall			
Network VLAN			
Latest Security O/S Patch			
Anti-Virus			
Unique Passwords			
Remote VPN Access			
Secure Data Server Room			
Public Wi-Fi			
Staff Wi-Fi			

(E) Policies & Protocols

	Yes / No	*Status*	*Comments/Type*
Public Liability Insurance			
Burglary Insurance			
Fire & All Risks Insurance			
Security Officer Protocol			
Visitor Access Control Protocol			
Denied Entry Signage			
Delivery/Courier/Mail Screening Protocol			
Unattended Item Protocol			
Cybersecurity Threat Protocol			
Telephone Threat Protocol			
Medical Response Protocol			
Services & Function Protocol			
Evacuation Protocol			
Daily Lockup Procedure			
Asset Register			

Security Survey Conclusion & Summary

A security survey will provide the HOW committee and/or security team with a direction in terms of which parts of the facility's security needs attention.

- Budgets are always limited and therefore security measures will need to be allocated based on the threats and vulnerabilities identified.
- It is important to have the buy-in of the HOW management team and involve the relevant stakeholders during your survey.
- The survey will consist of the following parts: **Initial Research, Data Collection, Site Visit, Interviews with HOW employees/management**, and the **analysis of Technical Data/Drawings**.
- Sites are dynamic, and after the initial survey, will need to be updated on a regular basis (audit).
- Your survey should include photos showing vulnerabilities, compliance issues, recommendations to improve security measures, and identified security failings in term of manpower, procedure, or protocol.
- The summary should include a list of priorities in terms of which areas need attention (critical/immediate, medium-risk, long-term/nice-to-have).

Section 3: Security in Depth

A critical goal for any security or emergency plan is to delay the perpetrator from access to the target/asset (the community) for as long as possible to allow time for law enforcement or security response to be activated to eliminate the threat.

The 2019 Yom Kippur attack on the Synagogue in Halle, Germany is a prime example of this. Physical barriers prevented the attacker from gaining access to the HOW community and denied him the ability to harm the congregants.

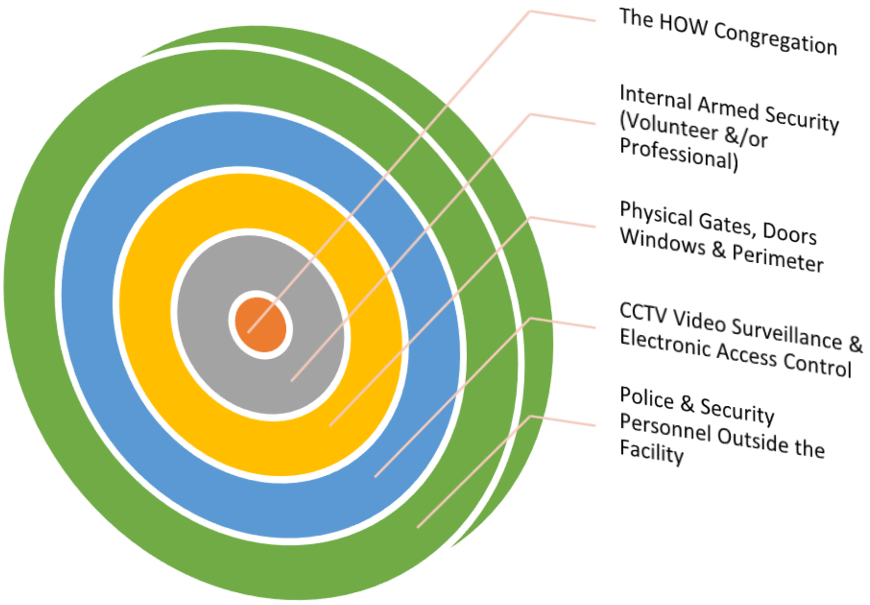
The Four D's

The ASIS principle of the four D's is a key component that should be applied in terms of planning countermeasures to protect the House of Worship:

- **Deter** – Implement measures to deter criminal or terrorist attacks against the facility.
- **Detect** – Detect suspicious or criminal activity early through man and technology.
- **Delay –** Implement physical security layers to delay physical access to the congregation.
- **Deny –** Deploy suitable response to the threat, i.e., community response or law enforcement.

Security in Depth

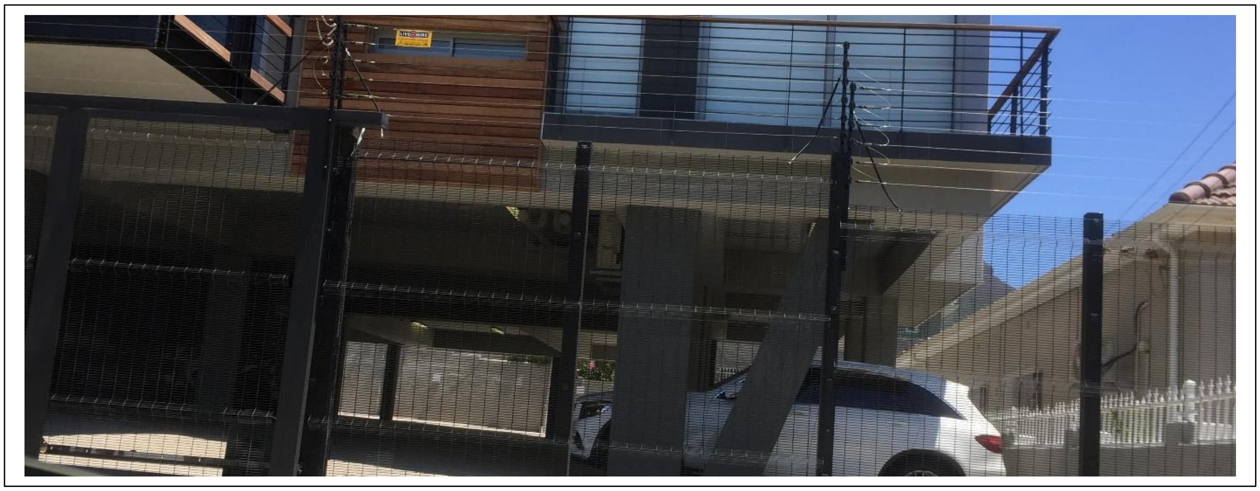
The community should not rely on a single security measure. They should always be implemented in layers as one measure may be overcome by the assailant. The concept of security in depth is very important; an example can be found below (one should compare it to the layers of an onion):


The HOW Congregation
Internal Armed Security (Volunteer &/or Professional)
Physical Gates, Doors Windows & Perimeter
CCTV Video Surveillance & Electronic Access Control
Police & Security Personnel Outside the Facility

CPTED

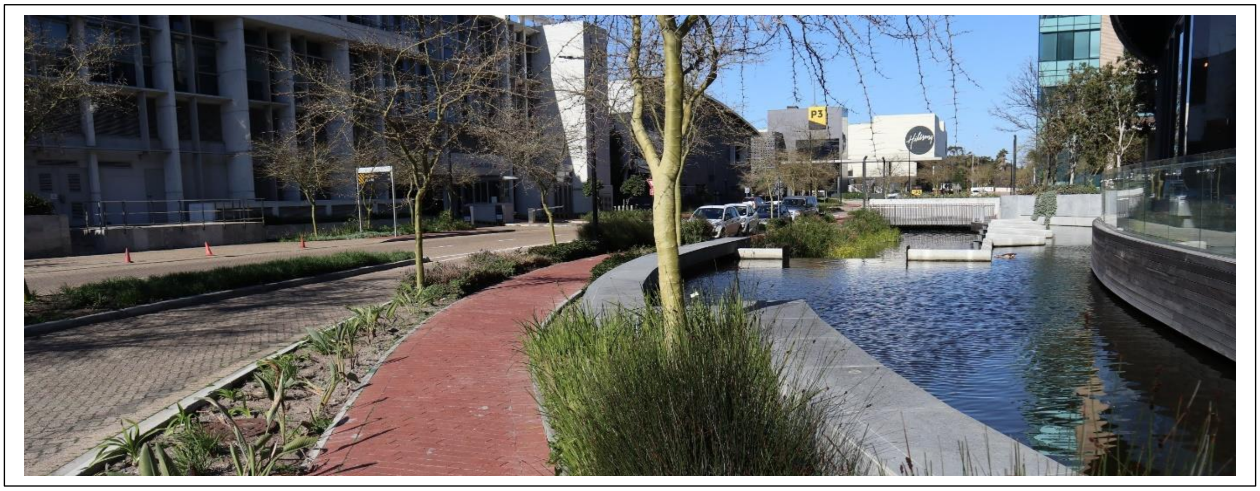
Crime prevention through environmental design (CPTED) is a concept that has been around since the 1960s and relates to the design of a site, building, or area to provide security through four strategies:

1. **Natural Surveillance** – Placing physical features, activities, and people to maximize visibility. This would include implementing physical measures which allow clear non-obstructed views of a facility, clear-view fencing, the use of glass, open spaces, good lighting, & low-cut foliage/trees. Don't always rely on technology to provide early detection of a suspect approaching the HOW.



See-Through Perimeter Fence = Natural Surveillance

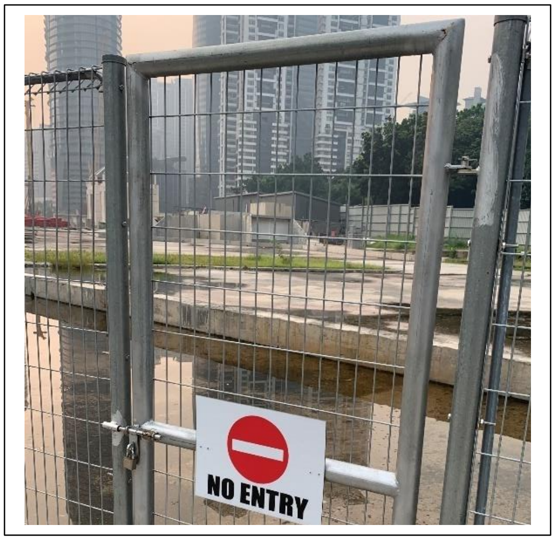
2. **Natural Access Control** – The placement of entrances, exits, pathways, paving, fencing, landscaping, and lighting. Facilities and garden landscaping should be designed to 'funnel' or direct individuals along certain access routes which can then be monitored by video surveillance or natural surveillance. It should also be aimed at clearly dividing 'public' and 'private' spaces, thereby discouraging certain individuals and risks away from the HOW facility.



Water feature acting as a natural barrier = Natural Access Control

3. **Territorial Reinforcement** – Using buildings, fences, pavement, signage, and landscaping to express ownership. As well as everyday objects such as plants, planters, and even an innocuous item such as a bicycle rack.

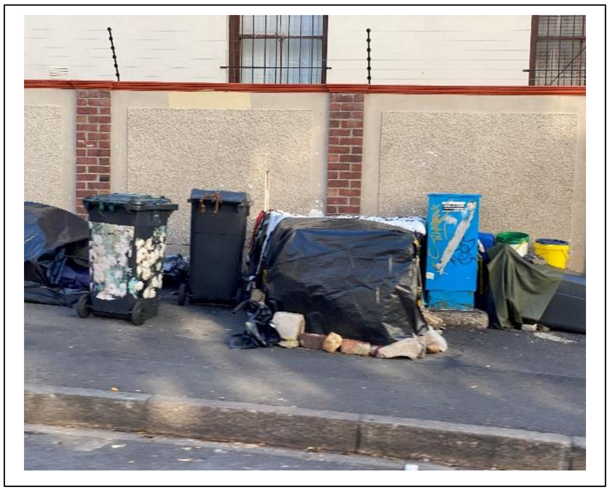
PROTECTED PLACE
保护区
NO ADMITTANCE TO UNAUTHORISED PERSONS
DI LARANG MASOK JIKA TIADA KEBENARAN
闲人免进
உத்தரவின்றி உள்ளே பிரவேசிக்கக் கூடாது
TEMPAT LARANGAN
பாதுகாப்பு உள்ள இடம்



4. **Maintenance** – Allows for the continued use of a space for its intended purpose. It also encourages the community to take ownership of the space and the positive image and atmosphere it creates. The broken window concept is also very important here.

   An untidy space often leads to anti-social behaviour, which eventually leads to criminal behaviour, which could impact the HOW and its community. This must include the eradication of graffiti, the improving of street lighting, social welfare programs for the homeless, and cleaning up and/or landscaping of areas. It is also recommended to engage the local council/municipality & community to be more involved in the maintenance of the overall neighbourhood. A happy community may lead to an overall reduction in crime.

   Especially consider CPTED when designing a new facility or doing upgrades.



Risk

There are five main ways of dealing with the risk facing a HOW facility which includes:

1. **Avoiding the Risk** – Not holding any HOW services (which would mean the adversary has won).
2. **Spreading the Risk** – As an example holding multiple services at different times or locations.
3. **Transferring the Risk** – This would involve the use of insurance policies by the HOW or the hiring of external risk management or security companies.
4. **Accepting the Risk** – Realising that risks are present and not doing anything about these.
5. **Mitigating the Risk** – Implementing additional security measures or 'hardening' the site.

Target Hardening

Involves the implementation of physical security measures to reduce or mitigate risk at a site. Many countries and states have programs that the HOW can apply to fund these measures.

Target hardening measures include:

- **Access Control & Intercom Systems**
- **Burglar Bars, Window Mesh, Pedestrian Gates, & Door Locks**
- **Intrusion Alarm Systems & Panic Buttons**
- **Perimeter Fencing or Walls**
- **Security Manpower**
- **Vehicle Bollards & Barriers**
- **Video Surveillance (CCTV) & Lighting**
- **Visitor Management (Electronic)**

Site Discretion & Disguise

A useful suggestion for protecting smaller houses of worship is that of discretion or disguising the facility as an everyday building such as a house or an apartment in a larger scheme. This is especially the case where the community is small and the threat to the facility/congregation is very high.

Discretion & Disguise – Planning

- Do not place any signage outside the facility.
- If video surveillance is to be used, keep it to the minimum and make sure it is discrete.
- Plan for internal courtyards where the community can socialize and celebrate.
- Plan accordingly for the community in terms of transportation to the facility or parking as to not attract unnecessary attention from neighbours.
- Ensure the entry point into the facility is suitably reinforced to provide the necessary delay.
- Discrete contact with law enforcement.

Discretion & Disguise – Operational

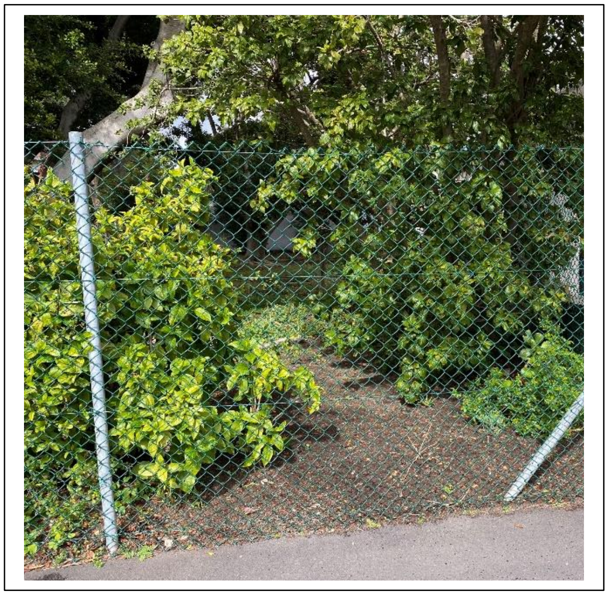
- No advertising of the address or times of service, etc. on social media.
- No loud music & no congregating outside the facility.

Fencing & Perimeter Walls

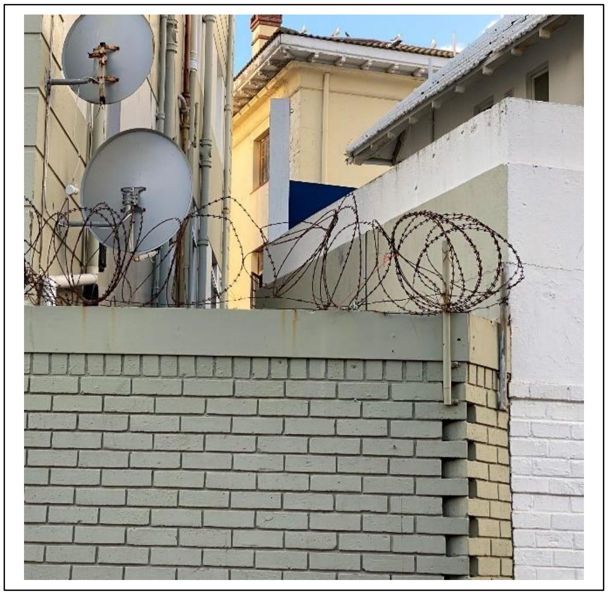
There are various types of fencing and perimeter wall structures that can be used to surround the HOW facility. These all serve two main purposes:

1. **Territorial delineation.**
2. **Act as a barrier to delay the intruder from reaching a target (community or other asset).**

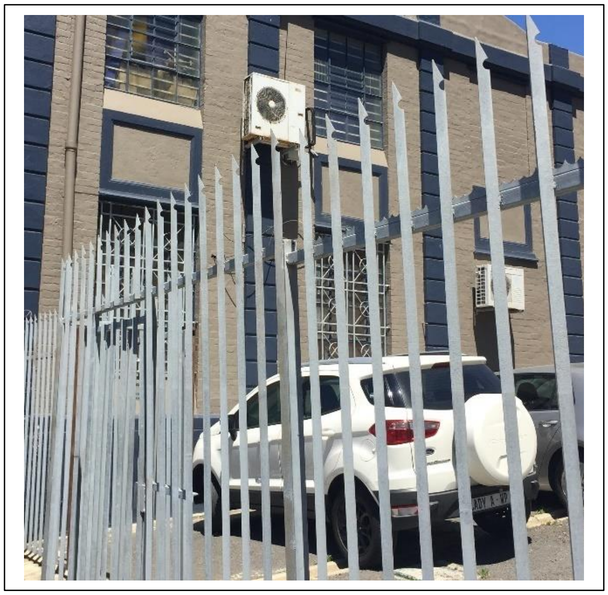
Various considerations need to be looked at when planning an upgrade to a perimeter. These include aesthetics, municipal, state or council laws, budget, foliage & landscape, maintenance, intrusion detection systems, electric fencing, anti-dig measures, anti-vehicle or IED protection, anti-climb measures, and the CPTED principle of natural surveillance.



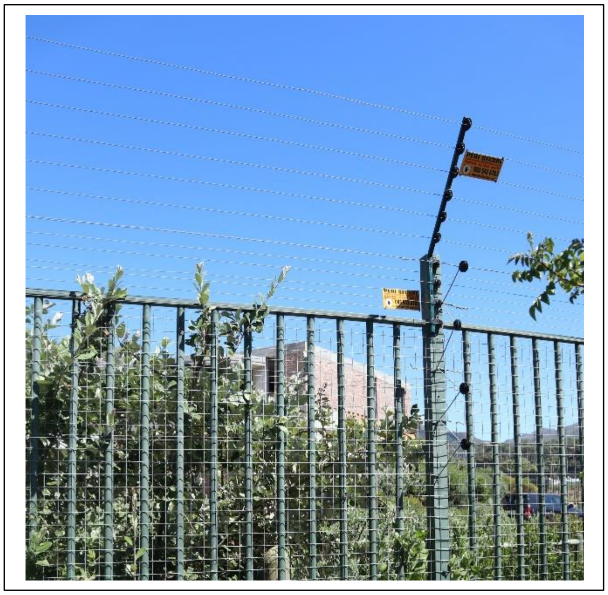
Diamond Mesh Fence



Brick Wall with Barb Wire



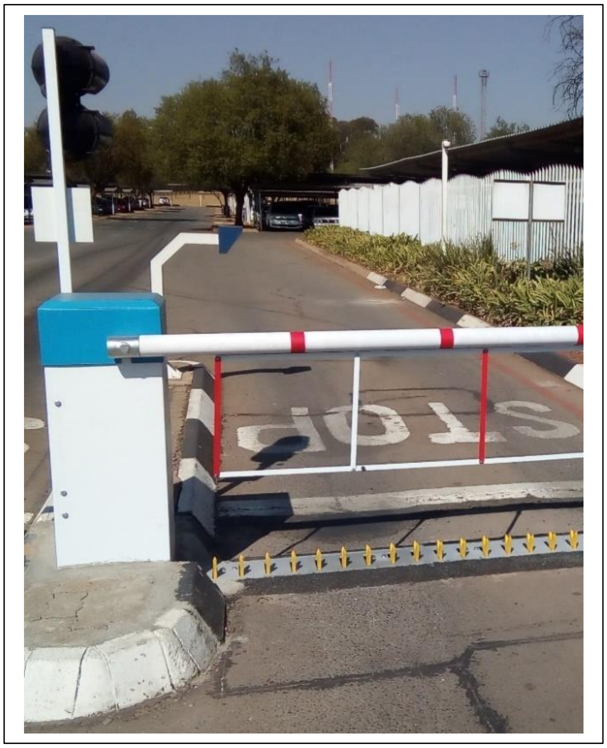
Devils Fork Palisade



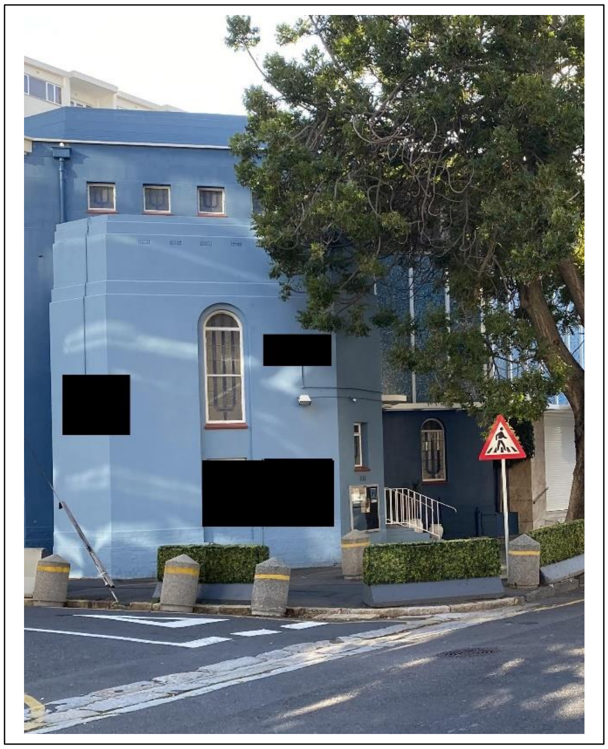
Palisade with Electric Fencing

Vehicle Barriers

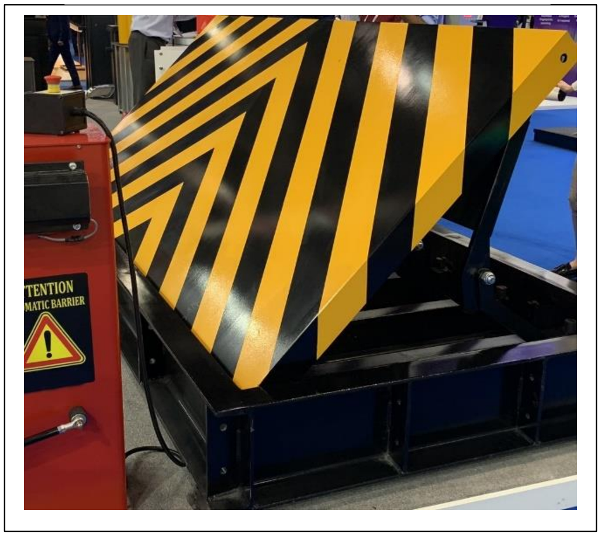
These help protect a facility against a vehicle-borne attack, either criminal or terrorist. They can be applied at vehicle entrances or around the perimeter of the facility to increase the stand-off distance between an attacker and the facility itself. Jersey barriers or heavy planters are relatively low cost and available either in concrete or plastic, which can be filled with sand or water. Temporary vehicle barriers such as strategically placed vehicles or equipment can also be used.



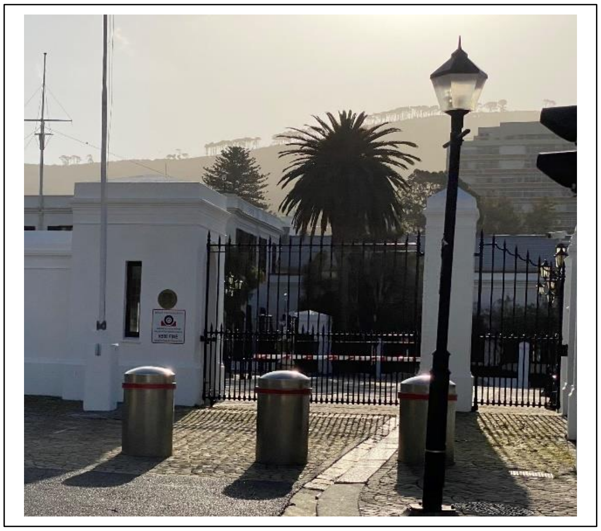
Vehicle Boom & Spike Barrier


[redacted]
[redacted]
[redacted]

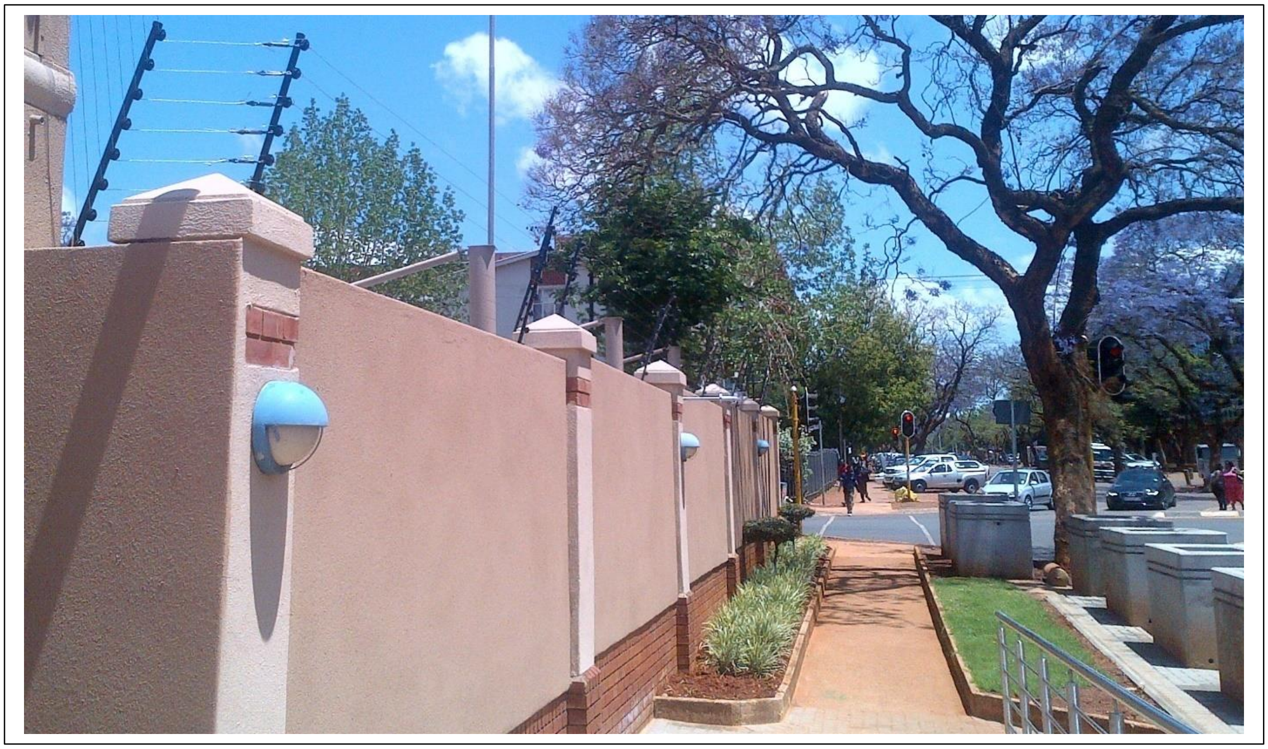
'Jersey-Style' Concrete Barrier



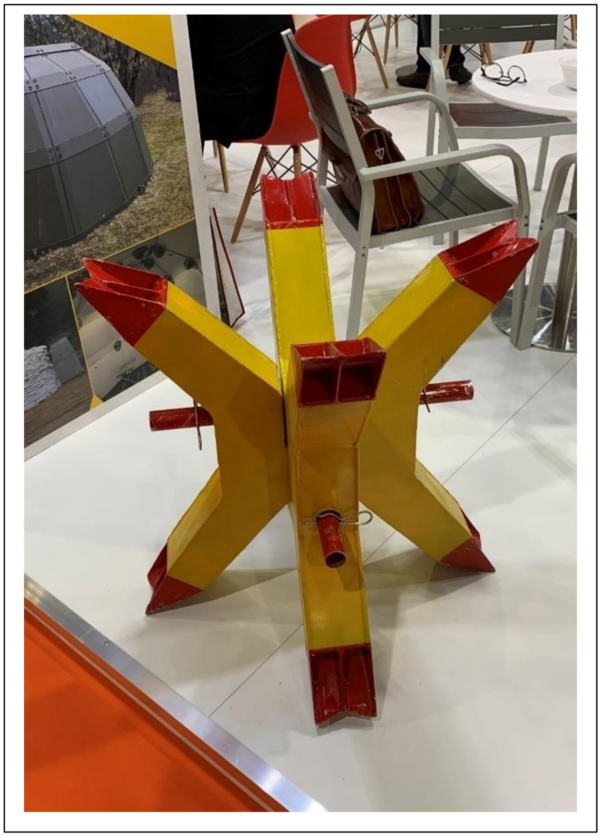
Pneumatically Raised Barriers



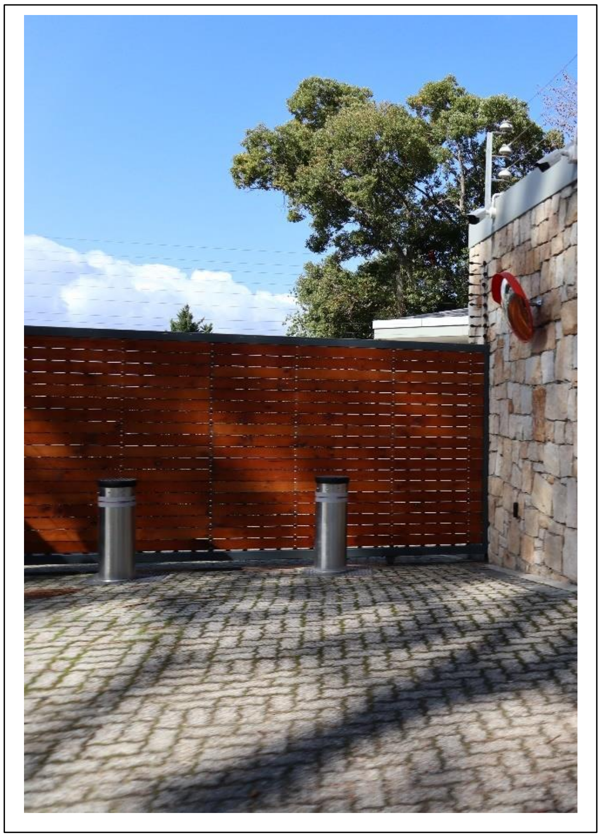
Fixed Bollards



Concrete 'Planters' to Protect Against Vehicle Attack & Provide a Stand-Off Distance



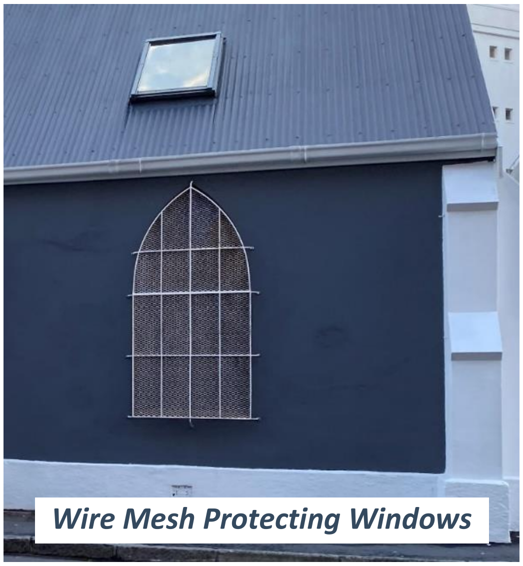
Portable Deployable Vehicle Stopper



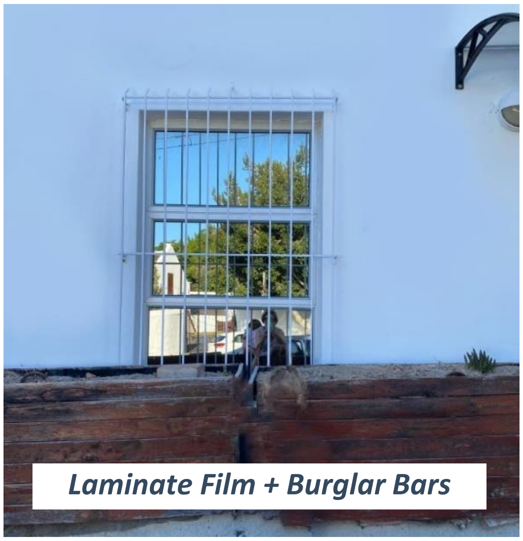
Pneumatic Vehicle Entry Bollards

Windows & Glazed Areas

- Building windows can act as entry points and can also potentially become projectiles in the event of an attack; therefore, they should be protected.
- The HOW should consider measures to protect the windows of the facility, both from intrusion, e.g., with burglar bars or mesh, but also to create a protective barrier, e.g., by fitting a protective laminated film.
- Where there is an increased risk consider replacing the exposed glass with laminated glazing, or if the risks are high, consider installing bulletproof glass.
- Another consideration is the use of tinting or a mirrored film, which can be effective during the day, but has the opposite effect at night where people can see in, but not out.
- Architects and designers should consider placing glass windows on the inside of a new building facing, e.g., a protected courtyard with the external side of the building a solid façade.
- If guard houses are necessary, bulletproof glass and intercoms can be considered to allow communication with visitors, contractors, or delivery staff.


Wire Mesh Protecting Windows

Unprotected Windows

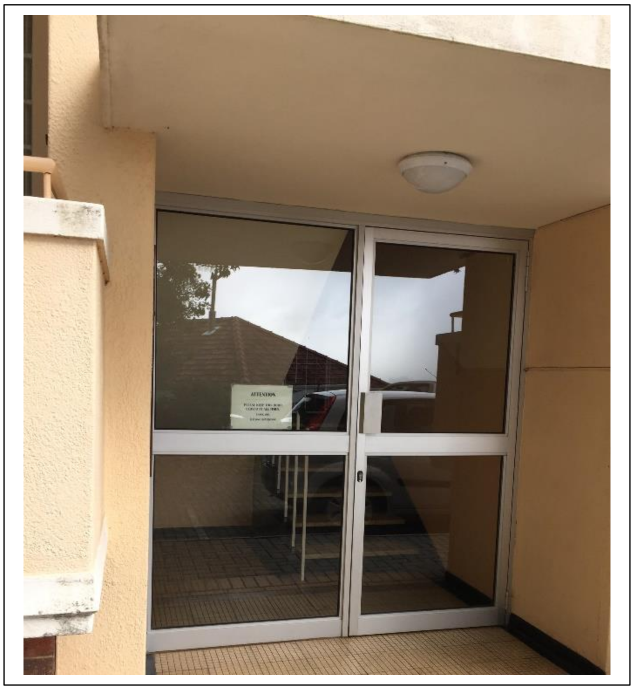

Laminate Film + Burglar Bars

Doors and Access Points

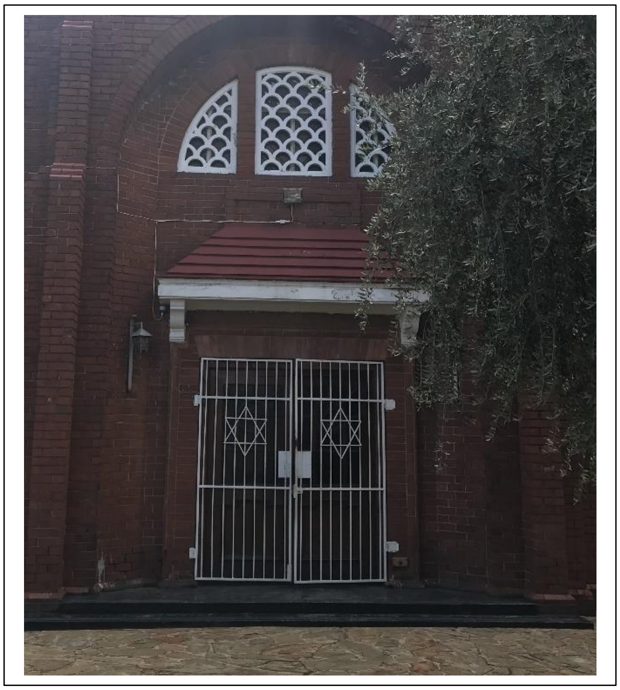
Doors leading into the place of worship are necessary to enable congregations to enter and depart. Unfortunately, they can also be the primary entry point for adversaries, either during services or when closed to the public. Internal doors provide delineation between public and private space which can include HOW offices, chambers, stores, and even safe havens.

It is therefore important to ensure, as far as possible, the following:

- Doors and gates are constructed using robust materials that will delay an attack.
- Suitable locking devices are incorporated to support the delay of adversarial entry. This should include the installation of at least two locking points on a door/gate, the use of locks that are less susceptible to crowbarring, and devices which can be used to secure an entry point quickly.
- Ensure allowance is made to facilitate surveillance through these doors such as with a peephole, surveillance camera, or viewing window.
- If glass is used as a door material, consider applying security rated laminates, or adding a metal security gate or metal burglar bar reinforcing.
- Internal doors segregating public/private space should have a form of access control (lock, access card, or mechanical combination (push button).
- Where the risks are very high, and a shelter is created, ensure that the access points are constructed of appropriate materials (i.e., security rated, ballistic sheeting).
- Ensure that escape routes are marked and easy to use, but still provide a robust level of protection from any adversary attempting to gain entry from outside.



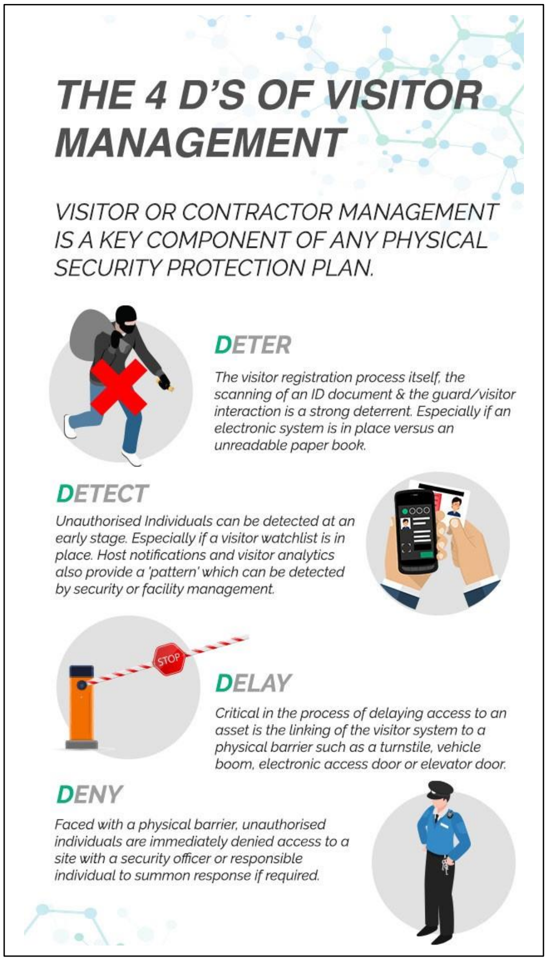
Good Natural Surveillance - But Physically Unprotected Door With Single Locking Point



Security Gate + Solid Wooden Doors + Dual Locking Points + Peephole

Access Control

Access control should be addressed as part of every HOW's security plan. Houses of Worship are meant to be inclusive and welcome to all, however, to raise security levels, physical access control and some form of a visitor management system may be required. The control of visitors, contractors, and delivery people in and out of your HOW is also very important.



THE 4 D'S OF VISITOR MANAGEMENT

VISITOR OR CONTRACTOR MANAGEMENT IS A KEY COMPONENT OF ANY PHYSICAL SECURITY PROTECTION PLAN.

DETER

The visitor registration process itself, the scanning of an ID document & the guard/visitor interaction is a strong deterrent. Especially if an electronic system is in place versus an unreadable paper book.

DETECT

Unauthorised Individuals can be detected at an early stage. Especially if a visitor watchlist is in place. Host notifications and visitor analytics also provide a 'pattern' which can be detected by security or facility management.

DELAY

Critical in the process of delaying access to an asset is the linking of the visitor system to a physical barrier such as a turnstile, vehicle boom, electronic access door or elevator door.

DENY

Faced with a physical barrier, unauthorised individuals are immediately denied access to a site with a security officer or responsible individual to summon response if required.

Access Control – System Design & Planning

- **When Power Fails:** Always consider how an access control system will function when power fails. Will the door open or will it remain closed? Will people still be able to gain access?

- **Local Authority**: Always follow local government guidelines, especially how one gets out of a building in the event of an emergency. As an example, are green emergency call points needed & for which control door side (safe or unsafe side).

- **Design for All:** Always cater for people with disabilities, e.g., correct mounting heights for card readers &/or intercoms. As well as providing a special needs gate @ a turnstile.

- **Select The Right Lock For the Job**: Always choose the correct lock for the door opening and if it should be fail-safe or fail-secure. Maglocks are not the solution for every door.

Access Control – Congregants/Employees

- During non-service times, the HOW facility can be fitted with some form of electronic access control for employees or congregants, although this may prove difficult to administer or manage.
- Gate/doors can be fitted with RFID card/tag readers, biometric readers, or wireless remotes with code hopping. Keypads should be avoided.

Access Control – Visitors

- Entrances into the HOW facility can be fitted with audio/video intercoms and CCTV video surveillance cameras that allow the screening of visitors by security or HOW staff.
- On entry, an area can be allocated where visitors can be processed accordingly (i.e., metal detector) and entered into a paper or electronic visitor register (if applicable).
- During service times this form of access control may not always be practical, and the HOW will then need to rely on volunteer or paid security personnel at entry points to conduct screening.

Alarm Systems

HOW facilities should be fitted with some form of alarm system, basic or advanced. When the HOW facility is in use, it can assist in providing a method for transmitting an alarm signal to activate some form of response (armed, medical, fire, etc.). Unoccupied, it will help deter and detect vandalism, fire, or theft.

Insurance companies may lower premiums for sites that have intrusion alarm systems installed, and many armed response companies (where permitted) provide a 'free' alarm as part of the monthly subscription service.

Alarm Systems – Planning

- An alarm system should be planned based on a security survey of the site and the guidelines for alarm systems from the local, state, or national government.
- If the budget and the site allows, external sensors can be considered as the first line of defense.
- Areas with excessive foliage should be avoided, cut back, or curtain sensors used in place.
- Main entrances into/out of the HOW facility should be fitted with both a door contact sensor as well as a PIR internal sensor. Trapdoors & roofs should be protected.
- Server rooms, safes, and cupboards storing valuables should be covered by the system.
- Avoid entry/exit time delays as these provide a risk to the facility especially if the intruder gets to the alarm transmitter before the system activates.
- Utilise alarm transmitters which have dual forms of transmission (such as radio, IP, and cellular).
- Avoid wireless alarm systems unless there is no other way to install the system. Wireless alarms are plagued by battery issues, reduced sensor range, interference, and 'sleep-modes' which helps reduce battery drain but shuts down the sensor after multiple activations.
- All sensors should be positioned to provide maximum coverage and have a minimum amount of false alarms.

Alarm Systems – Operational

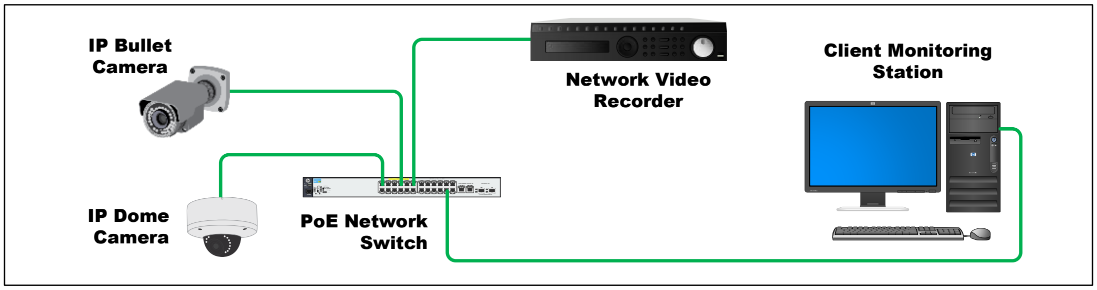
- **Individual User Codes:** Ensure individual codes are programmed for each alarm user. Avoid using a single blank code as this may cause issues in the event of an incident that needs to be investigated/audited.
- **Regular Maintenance:** Regular maintenance of alarm systems is important especially if the alarm system is wireless and/or regular power failures have been occurring in the area. This should include the testing of the alarm transmission device and all panic buttons.
- **False Alarms:** Can be caused by small animals, foliage, sunlight reflections, and pickup from neighbouring properties. Systems that have constant false alarms are generally switched off by their owners and put the facility at risk.
- **Reduce Security Manpower:** Alarms can help reduce security manpower requirements while the HOW facility is in use. This can be achieved by arming fire escape doors, perimeters, and unoccupied areas or buildings.
- **Arming/Disarming Notifications:** Ideally the alarm at the HOW facility should be connected to an SMS or IP transmitter to notify the HOW security team and/or management to an activation, panic alarm, or an opening or closing out of normal operating times.

Video Surveillance (CCTV)

Video surveillance is a security measure that can be used by a HOW at the site to provide the following benefits:

- **Deterrent factor:** A facility with visible surveillance cameras projects a vision of a hardened site.
- **Detection:** Live monitoring of a video surveillance system can be used for early detection of suspicious activity or a criminal act taking place.
- **Visual Alarm Verification:** On activation of an alarm, video surveillance can be used to visually determine the cause of the alarm. This can be helpful when the site is unattended or to monitor a vulnerable perimeter for intrusion.
- **Audit Trail:** An important tool for investigations as well as a backup tool to complement access control logs. The system can also provide evidence in the event of an incident.

A video surveillance system typically consists of the following typical components:



10 Tips for a Successful Video Surveillance New Installation or Upgrade

1. **Install Cameras Based on a Security Survey:** Camera placement should be made based on a security survey of the facility and the resulting set of needs. Don’t install cameras just for the sake of installing them.
2. **Place Cameras by Purpose:** Every camera installed should have a purpose and a required field of view, i.e., general coverage of the perimeter, coverage of the fire escape door, focused identifiable images of individuals entering, coverage of the vehicle roller-shutter, etc.
3. **Consider Lighting:** Cameras, regardless of the technology, need sufficient lighting to provide usable images. Facilities should not be recording the night-time image of a day/night camera as this lacks identifiable colour features (i.e., the suspect was wearing red pants & a blue cap).
4. **Choose a Suitable Recorder Location:** Depending on the size of the facility, the recording system should be placed in a central location to help cable distances, while at the same time balancing the need for a secure area with suitable ventilation or cooling. The recorder should also be protected from theft, vandalism, or unauthorized access.
5. **Scope of Work:** Ensure the scope of work is firm on the appointment of the installation contractor. This would include an agreed camera location drawing, an agreed recording retention period, as well as an itemized quotation with camera and equipment model number that will be supplied.
6. **Choose Proven Technology:** Be wary of overzealous camera salespeople over-promising solutions. Rather, choose a product which is proven and readily available from several sources.

7. **Cable Reticulation Planning:** The installer should carefully plan the cable reticulation, especially since many HOW facilities may be historical buildings. Consideration should also be made for future requirements such as spare conduit capacity or extra wire ways. All exposed cabling should be protected by conduit. Bosal metal for surface or PVC for buried conduit.
8. **Power:** As the old saying goes, power is the route of all evil. Steps should be taken to protect the electrical circuit feeding the HOW facility's video surveillance system. IP network video systems should have network switches and recorders protected by inverted based UPS units. 12VDC coax systems should have battery backup power supplies and UPS units for recorders. Dedicated circuits are best to avoid interruption of power caused by other electrical appliances.
9. **Video Monitoring:** The more people that watch video cameras the more effective it becomes. It also assists in early detection of camera faults. Video systems at HOW facilities should be placed in locations such as admin offices with the site caretaker, and if available, also in a security control room. The number of cameras being monitored should be kept to the minimum.
10. **Don't Overcomplicate:** Try and keep the system as simple as possible for the HOW. Complicated systems are costly to maintain, are never completed, and require constant adjustment by outside contractors. Video analytics systems have improved over the years, but a balance should be allowed for in terms of what is practical at the site and what works.

Unlike many commercial video surveillance systems, those required by HOW facilities often have a significant number of cameras covering external streets or public spaces.

- Apply for any public area CCTV permits (if applicable).
- Ensure video surveillance signage is in place to alert the public that recording is taking place.
- Ensure the HOW facility has in place a policy to handle requests for video evidence.
- Be aware of data protection requirements such as GDPR and how it impacts individuals.

Choosing the Correct Security Contractor for the HOW

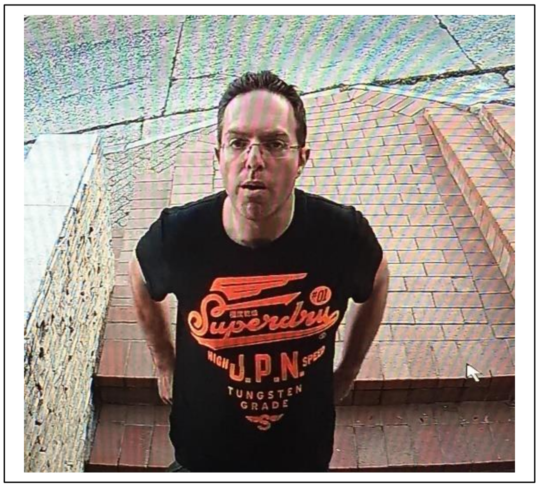
Various factors should be considered when choosing the appropriate security system integrator for your HOW facility, as the security costs spent need to last typically for up to 10 years.

- **Cost:** Be wary of selecting the lowest priced quotation, especially if there is a large difference in cost.
- **Accreditation & Insurance:** Ensure your selected contractor has the appropriate security accreditation, as well as public liability and site insurance.
- **Itemized Quotes:** Insist on an itemized quote which lists the make, quantity, and model of equipment offered for the project.
- **Conduit:** Cabling needs to be appropriately protected; query any quote which omits sundries such as conduit, trunking, or wire-ways.

- **Employees:** Avoid companies that make use of unvetted or temporary employees.

Video Surveillance Image Fields of View

To get the maximum value out of the video surveillance system, the HOW needs to achieve the correct field of view with the cameras that will be installed and balance capturing of details with situational awareness. Modern cameras have improved in terms of the pixels now captured, but camera lens angle and placement is still very important

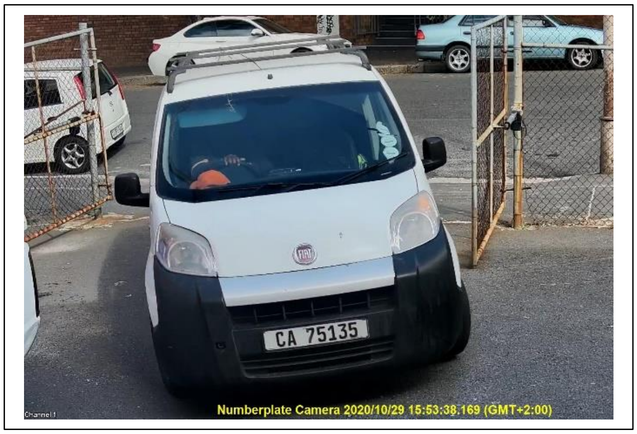


Narrow Angle Facial Entry Capture

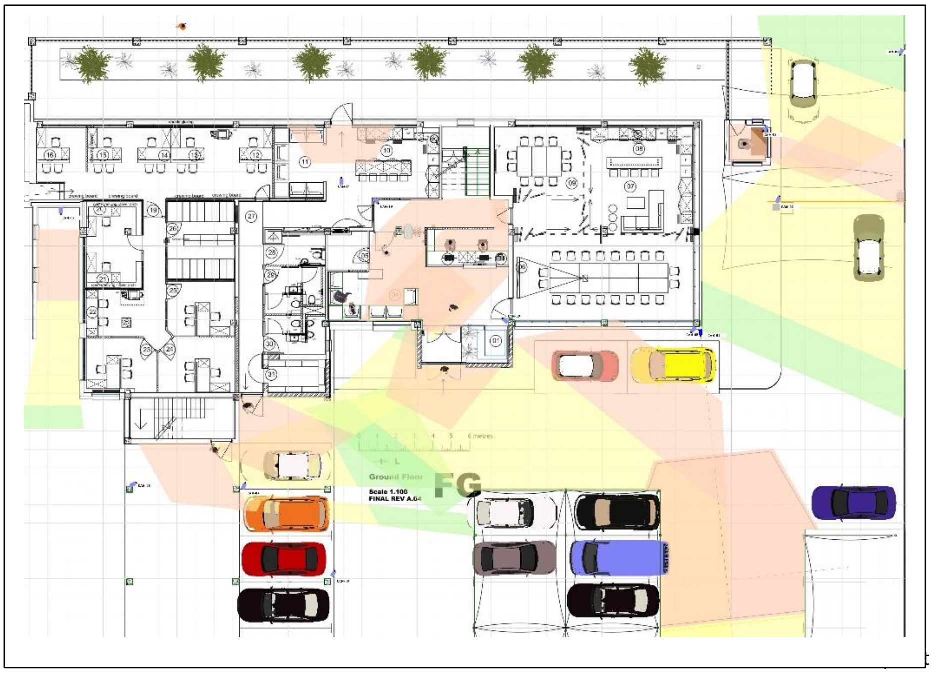
- Pedestrian or vehicle entry points are ideal **choke-points** and should have narrow-angle focused cameras to capture faces & vehicle details such as number plates. The use of masks post-COVID-19 does make facial capture more difficult.

- Wider angle camera views are useful for providing situational awareness, coverage of parking lots, identifying a chain of events and internal facility coverage.

- Perimeter cameras should be focused along the fence line and ideally cover both sides of the perimeter to pick up suspicious activity, information gathering, and possible intrusions. The HOW facility will also need to ensure the perimeter is kept free from foliage, that lighting is good, and that cameras cover each other to reduce blind spots.



Focused Vehicle Plate Capture



Modern 3D software modelling tools now allow one to accurately determine the best camera location, height and field of view for your facility. Red = Identify Unknown People. Yellow = Identify Known People, Green = General Surveillance of the Area.

Section 4: Direction, Control, & Communication

Direction and Control

Somebody should be appointed as the security responsible person for either the individual site or for the organization as a whole, which could include several houses of worship sites or facilities.

- Depending on the budget available, this could be a permanent employee or a volunteer.
- This person would be in overall charge of day-to-day decision-making regarding security, health/safety, and response. This can include addressing times outside of typical worship hours, such as office operations during the week, when an external group/organization is using the site, as well as security management during special events or functions.
- Other responsibilities can include security surveys, security audits, target hardening, volunteer recruitment, the general management of security personnel, and community training.
- They could also be the designated responsible person for emergencies and liaising with first responders, such as police, fire, disaster management, and emergency medical services.
- It may be appropriate and proportionate to establish an offsite control room (temporary or permanent) to act as an emergency JOC (joint operations centre for the community in the event an incident).
- This control room could include video surveillance feeds covering the various HOW facilities.
- It would also include communication systems to liaise with the community and local/national law enforcement, and/or emergency services.
- This would be influenced by the size of the community and available budgets.

HOW Communication

- Consider a point person who will liaison with the religious leaders and special groups within the congregation or community. They would become the HOW communication officer.
- They would be responsible for sharing information with the congregation before, during, and after an emergency, as well as general updates during times of trouble (such as pandemic).
- Information released by public address systems, newsletters, alerts via ushers, social media, or special smartphone applications.

Public Communication

- The HOW should appoint a member who will be the spokesman for the community to the media and have a clear policy in terms of information to be released.
- This person should have a calm demeanour, good speaking voice, and be experienced with dealing with the media and/or the legal aspects required thereof in terms of privacy, etc.
- Media channels would include the Internet, radio, television, and print.

Voice & Data Communication

- Planning should be in place to ensure the HOW has sufficient means to communicate. This would include 2-way radios, cellular communication, Internet connections, and/or fixed landlines.

Section 5: Cultural/Religious Sensitivities & Community Involvement

Different communities or houses of worship will have different cultural and religious sensitivities that differentiate them and make them special.

Cultural/Religious Sensitivities & Community Involvement – Planning & Prevention

- Any planning needs to cater to these and prepare community members for interaction with the HOW security team, as well as with law enforcement and/or medical services that would typically respond to incidents involving the HOW.
- This may include individuals of the opposite sex touching or interacting with the opposite sex in the course of an emergency.
- It may also involve certain individuals that have head coverings and certain communities that keep certain traditions or keep certain days such as the sabbath or other obligated holy days.
- The Orthodox Jewish community specifically prohibits the use of electricity and/or mechanical items on the sabbath. However, a dispensation is allowed under certain conditions to use them to save a life. This should be taken into consideration by the HOW security team.
- The use of guard dogs or explosive detection canines at mosques or shrines is a sensitive issue and needs to be discussed and/or coordinated accordingly with the community.
- Establish relationships with other faith-based organizations, as well as with the greater community at large.
- These coalition efforts should include harnessing available community skills.
- Educate members to act as **'force-multipliers'** by acting as the eyes & ears of the community (reporting suspicious activity, calling for help, & helping others, etc.).
- Identify any neighbourhood watch groups in the area and find ways to interact with them.
- Is there an active coalition or alliance of faith-based safety/security professionals in the area?

Cultural Sensitivities – Operational

- Houses of worship are encouraged to establish relationships with local law enforcement and other emergency response organizations.
- This can include inviting them for coffee/tea, scheduling training sessions, and/or meetings.
- Community members can become law enforcement or medical **reservists**. These individuals would provide a valuable bridge to the HOW community.
- Consider offering your HOW as a security exercise location so local law enforcement can become familiar with the HOW's layout, while at the same time sensitizing law enforcement to any unique considerations.

Section 6: Emergency Planning Around Children

Each HOW must consider the needs of children and other vulnerable populations will be met before, during, and after an emergency. Extra planning needs to be conducted to care for children, as they are dependent on adults for their safety, and their physical and psychological needs vary greatly depending on their age.

As a planning team develops procedures to care for children, the following aspects should be considered especially regarding HOW childcare, HOW camps, and/or religious schools:

- Establish procedures and protocols for emergencies when children are onsite or when they are off-site such as at youth camps, day trips, or HOW events such as choir competitions.
- Ensure those responsible for security and the off-site location (if there is one) have detailed emergency plans regarding the safety and welfare of children.
- Provide teachers or chaperones with contact information for individuals who could provide support or guidance while off-site (such as a nurse, counsellor, or doctor).
- Ensure your plan incorporates support for the children of HOW staff or volunteers to be cared for in an emergency if their parents or guardians have their emergency-related responsibilities (such as helping to lead the response).
- Purchase age-specific emergency supplies, such as medical equipment, and ensure who is responsible for maintaining them and who is trained to use them.
- Identify who will provide support in an emergency when children are on-site without their parents or guardians and who will lead and manage this response.
- Plan for child-focused training including infant or child CPR.

Teachers, childminders, or HOW employees should understand their role in an emergency (especially if they are directly supervising children), possible ways an emergency could affect children, and the importance of staying calm in an emergency to help keep children calm.

These staff members should also be fully aware of the procedures for how to release children to a parent or guardian and who they should contact if they have any questions or issues.

Data Capture & Credentials

- It is important to establish how information on parents or guardians will be recorded (e.g., when children are first registered) and stored, such as who can pick the child up, who to contact in an emergency, and whether the child has any allergies, as well as how this information be reviewed and updated if necessary and at least annually.
- The HOW facility could also consider electronic visitor or access control systems that could be used to scan a credential held by the parent or guardian when a child is collected.
- The same device could be used to scan a QR code or RFID tag attached to a child's bracelet or badge to establish identity or retrieve emergency info.

Visual Aids

Visual aids are helpful for HOW staff in an emergency. These would include evacuation route maps, checklists of what to do in an emergency (e.g., evacuate, shelter-in-place, or lockdown), and emergency contact information posted in convenient locations around the HOW facility.

Communication

Allocate somebody to be responsible for communication with families in an emergency about their children (e.g., whether the child is on- or off-site, injured, missing, etc.)

Consider sharing, with parents or guardians, information about expected actions in an emergency.

Evacuation

- Establish the primary and back-up locations that children will be moved to after an evacuation.
- Plan how children who are too young to walk will be transported, such as through the use of cribs that can be rolled out of the building.
- Ensure classrooms are double-checked to ensure children are not left behind (some may be scared and hiding).
- Establish who is responsible for taking emergency supplies in an evacuation (e.g., contact information for parents or guardians). This reinforces the idea of using a portable electronic registration system and is used away from the main HOW facility.
- Work out how children at the rally point will be accounted for and what are the procedures if a child is missing or injured.

Shelter-in-place

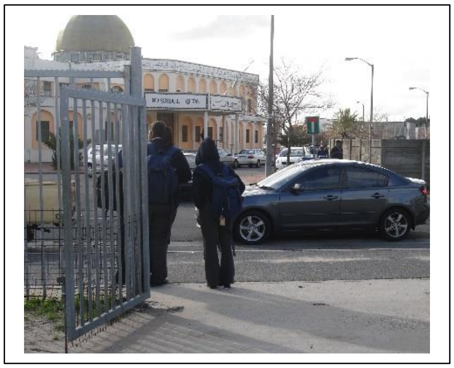
- Consider supplies of toiletries, snacks, bedding, and water to shelter-in-place.

Lockdown

- Work out how doors are locked or barricaded to prevent somebody from entering the room.
- Should children be shown how to operate these in the event of an adult being incapacitated or missing?
- Establish the best way for children to be hidden inside the room so they're not visible from outside.

Family Reunification

- Consider what protocols need to be created to reunify children safely and effectively with their parents or guardians after an emergency incident.
- What separate location (where the flow of children and parents/guardians can be controlled) can be used for family reunification, if needed, and how will families be made aware of the location.
- How can emotional and psychological support be provided to families in the reunification area?
- Establish who should be informed (e.g., law enforcement) if children cannot be reunified with a parent or guardian and at what stage of the search.



Section 7: Training, Volunteers, & Exercises

Volunteers

Volunteers are an essential part of any HOW security and emergency plan.

They often form the main part of the HOW security manpower.

- The volunteer program needs to be run in a professional and organized fashion.
- Volunteers should be made aware of the responsibility involved and ensure they can commit sufficient time for operational work as well as training and scenarios.
- The HOW should ensure the volunteers follow the law and are accredited based on local/national government guidelines in terms of security and/or medical work.

The Community as Force Multipliers

Any security plan should include the use of the community as a security force multiplier.

This would include:

- Assistance with training.
- Assistance with fundraising.
- Assistance with security awareness campaigns.
- Assistance with legal issues, legal reviews, & contracts.
- Reporting of suspicious individuals, vehicles, or activities to the HOW security team.
- Reporting of security measure vulnerabilities to the HOW security team.

Training and Exercises – Planning & Prevention

Any security plan should include elements learned through training and regular security exercises (whether they be tabletop, medical, fire drills, live exercises, or others).

Among the points to consider in developing training and exercise programs:

- What training and exercises will be conducted to ensure successful prevention, mitigation, and response, including how often they will be conducted, and who will be involved.
- Types of threats applicable to the place of worship and how to recreate these with training.
- Addressing the threat applicable to every form of HOW, including the threat of sexual and/or physical abuse to children or at-risk adults.
- Syllabus of topics/content to be covered in any training program.
- These may include security basics, first aid training, self-defense, counter-surveillance, weapons training, and access/control screening.
- Review training materials and equipment regularly.
- Invite guest lecturers on specialist topics.
- Encourage volunteers to join emergency and law enforcement volunteer programs as volunteer EMTs, firemen, auxiliary, or reservist police/law enforcement.

Emergency Medical Scenario Training

Training – Operational

- Conduct regular training sessions with HOW volunteers & employees.
- Revise as and when needed with feedback from management, volunteers, & employees.
- Keep a written record of all who have participated in the training.
- Conduct live drills and/or scenario-based exercises coordinated with local authorities, if possible.
- Have actors with instruction to simulate probable activity.
- Evaluate drills and implement corrective action as needed.
- Consider a simple fire drill at one of the services as an example.
- Encourage volunteers to participate in medical, law enforcement, & firefighting programs to gain experience and camaraderie.
- Incorporate all lessons learned during training, practical work, and exercises in the proposed security plan and its updates.

Emergency Medical Evacuation Training Exercise

Section 8: Planning Private Security Manpower

Dedicated security personnel may be an important part of the HOW security and emergency plan. Some facilities may have paid security staff, while others may rely on volunteers or a combination of the two.

Before enlisting the services of a security company, various factors should be considered:

- **Accreditation:** The guarding company should be appropriately registered or accredited with the appropriate authorities and/or legal bodies in that country, state, and/or local jurisdiction.
- **Insurance:** The security company should have the appropriate insurances in place. This could include public liability insurance, vehicle insurance, etc.
- **Budget:** The lowest quote should not always be accepted, and other factors should be considered in conjunction with the price.
- **Company Infrastructure:** It is important to look at the security company's infrastructure. This would include the availability of a control room, number of supervisors on the road, armed response backup, and other services that the security company can provide.
- **Security Company Size:** It is not always the size of the company that matters, it is the management that is critical. Some larger companies may have so many clients that there is a loss of personal service. An owner-managed business with appropriate resources should not be discounted in the evaluation.
- **Locality:** Certain security guarding companies will have a better presence in a certain area than other companies. This would increase the number and length of visits by a security supervisor: it may also mean they have a better relationship with local law enforcement and/or emergency personnel.
- **Equipment Issued:** The deterrent factor provided by uniformed security staff is an option for the HOW site to consider. A properly uniformed officer with the appropriate equipment may help deter a perpetrator.
- **Non-Disclosure Agreement:** The HOW should consider having the security company sign a non-disclosure agreement both in terms of the company & the employee. This may prevent the leaking of confidential (such as vulnerabilities) or private information from the HOW.
- **Staff Selection Process:** Besides the management of the security company, the selection process used to select personnel is probably the most important aspect to consider. Companies with a high turnover of staff or with a poor selection process should be avoided at all costs. The security company must liaise with the HOW facility to ensure the correct personnel are placed at the site & limit staff turnover.
- **Training:** Does the security officer have any training that would be helpful to the HOW, i.e., firefighting, first aid, health/safety, firearms, etc.
- **Contract Length:** Be careful of contracts which lock the organization into a long contract period.
- **Manpower Selection Criteria:** Any selection criteria should include the checking of the following for both the security company as well as the personnel to be deployed (in an ideal world):

  Criminal Record, History of Sexual Assault, Mental Health, Physical/Medical Fitness, Reliability & Time/Keeping, Medical or Firefighting Skills, Law Enforcement Experience, History of Drugs or Gambling, Credit Check/Credit History, Social Media, and Political Affiliations.

Section 9: Armed or Unarmed HOW Security

Please note this section refers only to jurisdictions where the private carrying of firearms is allowed.

A big question every facility will ask is whether or not the facility will have armed security.

One needs to consider carefully if the armed security will become a risk to the HOW or if it will be an asset.

It may be better to improve the physical security at the site rather than introducing a person that may inadvertently injure a member of the community due to poor training, friendly fire, or lack of experience.

However, sometimes an armed volunteer, congregant, or security officer may be the only thing standing between the congregation being injured and the waiting time for law enforcement responding.

Therefore, various key factors need to be considered including:

- **Availability of Armed Law Enforcement:** If a threat is identified and the use of firearms is required to protect the facility. The first port of call should be to approach the law enforcement in your country, state, or region to see if they are available to assist with armed security for the HOW facility. In many countries, only the police or army can provide armed security.
- **Training:** Any armed person at the HOW should have the appropriate firearms and tactical training as they may well find themselves facing a target in a crowded room. This may include an individual who has SWAT or advanced military training.
- **Experience:** The armed person should have the necessary experience in operating in hostile or operational situations. This may include active-duty law enforcement personnel.
- **Concealment:** The HOW should consider having the armed security as an undercover person who is only used in the event of an attack on the facility. In such a scenario, unarmed uniformed security could be used to tackle other everyday security scenarios. This would be very helpful in mitigating the threat of an active attacker.
- **Budget:** A very important factor is whether or not the facility has the appropriate budget to procure the services of an appropriately trained and experienced armed security person.
- **Legal:** The HOW should always follow the law of the state or country they are resident in. This may include the appropriate accreditation, carry permits, firearm competency, and the required insurance. A legal defense plan should also be in place for a situation post an incident.
- **Insurance:** Ensure that your insurance carrier is aware if you are going to utilize armed personnel as part of your security program.

- **Terms of Engagement:** Terror versus criminal incidents. Would they be handled in the same manner, as the risk to the community is the same at the end of the day?

Section 10: Threat-Specific Emergency Scenarios

It is very difficult to predict how people will react to an emergency.

It is important to:

1. **Plan, train, & prepare for emergencies.**
2. **Be aware of your surroundings.**
3. **Call for help.**
4. **Try and remain calm.**
5. **Help others.**
6. **Fight the fight or fight the fire.**
7. **Escape or shelter in place.**
8. **Restore the HOW to normal and carry on life.**

Active Attacker

- Response training to an armed attacker (firearm, knife, or other weapons).
- If the risks dictate, consider issuing community volunteers with anti-stab or bullet-proof vests (overt or covert in nature).
- Protocol for intervention-capable & non-intervention members of the HOW response team (including the use and carrying of firearms and/or less-lethal weapons if applicable).
- Individual HOW needs to adopt a training response model that is fit for purpose and within the accepted norms of the country where the HOW is located.
- Implement physical barriers to increase the delay of the attacker getting to the community.

Arson Attack

- Address arson with a focus on preventive mitigation measures.
- The use of video surveillance to capture areas of the facility that could be at risk of arson.
- Assess if the perimeter of the facility/site will help protect the building from approach by the arsonist.
- Ensure the facility or HOW has a suitable fire detection system and it is operational.
- Ensure the facility has the correct cause and effect process in place in terms of the fire system; this may include the activation of warning lights, sounders, sprinklers, and notification transmission to either a security company or directly to the fire department.

Armed Robbery

- A reality in many communities is that of armed robbery hold-ups.
- Valuables carried by community members may be targeted or the collection money/tithes collected each week by the congregation.
- The site should consider and act appropriately to safeguard the community.
- Ideally, the congregation should have access control, both in terms of manned visible security screening, as well as electronic security gates and/or doors (if possible).
- Many congregations that collect large amounts of cash have counting rooms, drop-safes, and hi-security doors protecting these rooms.
- Armed or unarmed security can act as a great deterrent to armed robbery.

- The congregation could consider steps to reduce this risk by accepting non-cash donations, having congregants do bank transfers, and advise the congregation to leave valuables at home.

Building Compromise

- Plan for what to do if the building is inaccessible due to conditions inside or outside the facility.
- Plan for a response in the event of a building collapse (could be caused by a man-made risk such as an explosion or natural risks such as by earthquake or storm).
- Know how to respond to a building or site fire, including warnings or notifications (e.g., fire alarm), and what resources (human and material) are available to extinguish a small fire.
- Develop protocols for the HOW security team to activate the required medical, fire, &/or civil response.

Bomb Threats

It is recommended that a bomb checklist be placed near all incoming phones and those who answer phones be trained to use this checklist.

- Ensure sufficient information is recorded by the call-taker and ask as many questions as possible. This may include the caller's voice or accent, background noises, behaviour, the wording of the threat, caller's name, time of the activation, what type of device, where the device is located, and anything that may aid law enforcement in the investigation.
- Notify law enforcement and any dedicated security personnel there are.
- Have a procedure in place in terms of evacuation, lockdown, and community communication.
- Consideration should be given to awaiting law enforcement or security response before evacuation to ensure the safety of evacuees once outside of the building.
- Keep in mind that during evacuations, terrorists can place IEDs in likely evacuation routes or points.
- Take note of any visible suspicious packages, items, or vehicles (HOT principle).
- Do not tamper with or touch this suspicious item and/or the vehicle.
- Seal off immediate areas to prevent the community or the public from proceeding into danger.
- Move away from the facility and away from any potential hazardous debris such as glass windows and/or flammable items.

Muggings/Street Robberies/Vehicle Break-Ins/Isolated Attacks

- Educate the community as to crime trends & the avoidance of having valuables on show.
- Extend the security bubble out during the arrival of the community, retract it during the service to protect the facility, and then extend it out again during egress.
- Arrange for law enforcement or security vehicle patrols during times when the HOW is in use.
- Encourage the local council to improve street lighting, promote community patrols, and uphold relevant bylaws (such as loitering, anti-social behaviour, etc.)

Pandemic (Such as COVID-19)

- Ensure solid communication within the community to update them on government guidelines and protocols for returning to the HOW.

- Identify vulnerable HOW community members and develop appropriate protocols for their care. This may include the elderly, medical personnel facing regular exposure, and HOW members suffering from chronic illness.
- Establish objective, guideline-based protocols early to determine the criteria for safely returning to the HOW.
- Develop guidelines on how to handle HOW members who ignore, resist, or reject HOW guidelines in place for pandemic transmission mitigation.
- Implement screening protocols for any community members entering the facility, as well as the handling of members who may present with symptoms.
- Ensure the correct PPE is in place and is being used by employees and/or the community.
- Implement protocols for the cleaning and disinfecting of areas and the facility.

Social Unrest, Anarchists, & Demonstrations

- Communicate any issues or risks to the community and act accordingly in the holding of services should the political environment be deemed a danger to the HOW's congregation.
- Considerations can include riots, protest marches, service delivery action, or other political incidents such as a coup d'état.
- Protect windows, glass panels, and or decorative art or facades through the use of non-descriptive wooden or protective hoarding.
- Lock away or relocate irreplaceable objects of value.
- Ensure video surveillance is in operation to capture potential perpetrators of violence against the facility.
- Communicate with law enforcement and the external community as required.
- Be prepared to remove or secure paper documents containing sensitive or personal information. Any such documents should be destroyed in such a way so they cannot be reconstructed.
- Be prepared to remove and secure all IT related equipment including computers, storage media (USB sticks, virtual drives, etc.), routers, etc. Suspend Internet access with the service provider to prevent unauthorized or illegal usage. Change passwords on any cloud-based drives and consider destroying particularly sensitive storage media (e.g., anything containing HOW member names and addresses, financial information, HOW leadership meeting notes, etc.).

Vandalism/Burglary/Desecration

- Ensure mitigation measures are in place to prevent this, including target hardenings such as alarm systems, video surveillance, perimeter fences/walls, gates, and security patrols.
- Consider risk transfer measures such as facility insurance.
- Ensure the community reports all incidents to the HOW security team.
- Report any incident to law enforcement.
- Report any incident to your neighbourhood watch group, local council, or local government.
- Photograph and record any evidence (if applicable).
- Ensure a protocol is in place for those that will be responsible for cleaning/repairing/restoring.
- Have the HOW communication officer deal with the media and/or the community.

Suspicious Items & Evacuation

A major concern at a HOW is that of unattended or suspicious items. These could turn out to be something completely innocuous or could potentially be a great risk to the HOW facility and its congregants. The key here is the way the HOW handles the incident and the steps that precede the incident.

- **Step #1** should be community awareness training or programs on educating the HOW community not to leave items unattended and what is appropriate to bring to the HOW service.
- **Step #2** should be a prescreening of the facility before the service/function starts and the identification of any known or unknown items. It would include an outside-inward approach and would cover the exterior of the facility including vehicles, utility areas, and foliage.
- **Step #3** should be a screening/searching process when HOW community members or congregants enter the facility. This would include people carrying inappropriately sized baggage such as suitcases, etc., and denial of individuals bringing gifts/goods on behalf of others.
- **Step #4** should be the location of the unattended item and the cornering off of the area to prevent the community and/or individuals from entering the space.
- **Step #5** should be to use the community to quickly assist in finding the owner of the item.
- **Step #6** should relate to evacuating the area and calling the appropriate law enforcement body. This would affect the way of life of the community & needs to be carefully considered.
- **Step #7** is the work to be done by the HOW communication officer in giving feedback to the community post-incident.

Suicide Bombing Attacks

It is unknown what motivates suicide bombings beyond being forced into action by others using brainwashing and ultra-hatred for the target of the attack. The result of these attacks is often devastating both in terms of loss of life but also the impact against the targeted HOW.

- Go back to the 4 D’s principle. The suitable delay should always be present in the HOW security plan in terms of law enforcement warnings, security screening, and blast protection.
- A close relationship with law enforcement is essential to provide the necessary warnings and/or intelligence before an event. No warning should be ignored.
- The HOW should be ultra-vigilant against individuals who appear to be acting out of the ordinary (behavioural indicators such as not responding to verbal commands, red eyes, sweating/pale), wearing unsuitable bulky winter clothing in summer, and who are carrying luggage into the HOW. Both men and woman should be considered a threat.

Vehicle Ramming Attacks

- An increasingly used terrorist attack method is using a vehicle as a weapon against pedestrians.
- To protect against vehicle ramming attacks, vehicle barriers protecting sidewalks and/or entrances is essential and provides some protection for pedestrians.
- Barriers could be in the form of pneumatic ramps, motorized bollards, water-filled temporary barriers, concrete barriers, special spikes, or even innocuous concrete planters.
- Keep the congregation off the sidewalk and in a covered controlled space.

Section 11: Medical Emergencies

Medical emergencies in HOWs are probably more common than security emergencies, and the security team and/or responsible individuals must be aware of what to do in the event of such an occurrence.

This should include how to respond to various medical emergencies—from minor to major—including who is medically trained/certified to respond, where resources (e.g., AED, oxygen, doctor, medic) can be accessed, efficient communication with and the prompt activation of community, state, and private medical responders.

Emergency Medical – Planning & Prevention

- Emergency response readiness (location of emergency medical equipment, emergency vehicle approach, parking, and egress).
- Community CPR, first aid training, & basic trauma life support training.
- CPR protocol posters & medical response telephone numbers should be posted at key locations around the HOW facility. This should include national emergency numbers.
- Identification of available community resources and/or volunteers (doctors, nurses, emergency medical technicians, paramedics, etc.).
- Identification of appropriate medical facilities in terms of proximity to the facility.
- Procurement of and/or servicing of the site’s emergency medical equipment.
- Identification of those holding CPR and first aid certifications, and the posting of these lists in key locations (nurseries, classrooms, beside first aid equipment).

Emergency Medical - Operational

- If all else fails in an emergency, stick to your medical and CPR protocols. As an example (hazards, hello, help, airway, breathing, circulation, disability).
- Calling for help early on in the medical emergency is key, as is proper instructions in terms of activating the medical response and advising them as to the patient's condition, the number of patients, correct address for the facility, adjacent landmarks, & the best route to the HOW.
- Most countries have a central emergency number that can be used to activate help from public services such as **911** (Argentina, USA, Mexico, & Canada), **112** (Europe & South Africa), **999** (Britain, UAE, Saudi Arabia), **000** (Australia), **111** (New Zealand), **100** (India), **110** (Japan).
- However, certain countries may have private medical response companies that are quicker in responding, but government/public medical services should not be ignored as they have the weight and resources of the country at their disposal, including medical rescue, disaster management, medical air services, and specialist emergency response doctors.
- Fire departments are also a valuable resource to tap in terms of quick medical response. They are often area bound and have a medical response service close to many urban areas or in rural areas where a volunteer fire service is based.
- The key is to get a quick emergency medical response to your HOW facility with the appropriate means of ambulance transport (road or air) to the most suitable emergency medical facility.

- Assigning community members to prepare the area/site for the arrival of the medical response team and providing an escort to the location of the patient.
- Promote basic trauma and medical treatment skills amongst the community and make use of medically trained volunteers.
- Always protect the patient’s privacy and the confidentiality of any medical information in your care during or after a medical incident (e.g., specific symptoms, medications, comments made by first responders, etc. (as an example, if a person has COVID-19 symptoms).
- Appropriate handover to the medical response team (patient history, a brief rundown on the incident, and any other relevant information).
- This will most likely be the decision of the senior medical practitioner on the scene, but it is always best to ensure the patient is transferred to the appropriate medical facility.
- If all else fails then to the closest hospital with an emergency unit.
- Plan what to do in the event of the death of a community member or a member of the public.
- Develop a notification process for family members/emergency contacts of the injured person(s).
- Ensure continuous ongoing community training (CPR training, first-aid training).

Section 12: Cybersecurity

Because of the COVID-19 pandemic, the Internet has taken on a key role in the life of a HOW. Most HOWs now rely on online conferencing services, social media, and other services to host meetings, conduct meetings and studies, and communicate important information to their congregants. The ability to respond to the unique online threats posed by this rapid shift may vary greatly depending on the resources available to a HOW leadership team.

Regardless of size, however, every HOW needs to ensure they have a robust policy and measures in place to protect not only their “connections” but the data entrusted to them by its members.

Cybersecurity – Planning & Prevention

- Ensure the facility has basic IT security measures in place and an IT security policy document, which all employees/volunteers need to sign.
- Implement an awareness campaign to discourage users from using porn sites, gambling sites, and/or the use of torrent downloads using the HOW’s IT network.
- Part of this should include awareness of opening unknown files or clicking on links sent by unknown senders.
- Each facility should have a suitable firewall Internet router for the facility’s Internet connection as well as the installation of antivirus software on facility computers.
- Identification of cyber threats which may include phishing attacks, denial of service attacks (DODs), network hacking, or interception of emails.
- These could be both a security threat and/or a financial threat to the HOW facility.
- Security measures would need to protect community databases, especially those in terms of financial donors to the community (customer lists).
- Attempt to locate all IT equipment in a secure server room, which is lockable, with restricted access, suitable ventilation, and appropriate power backup.
- Consider migrating onsite applications such as accounting systems, databases, and email to the cloud to reduce the risk of data loss in the event of an issue onsite.

Cybersecurity – Operational

- Apply regular operating system and application updates/security patches.
- Regular Wi-Fi password changes.
- Use strong passwords for employee & guest Wi-Fi, video surveillance recording systems, access control systems, PC operating systems, accounting systems, and HOW databases.
- Do not disable anti-virus or firewall to overcome PC installation issues.
- Ensure video conferencing events have appropriate password protection.
- Continuous cybersecurity awareness training for HOW staff/volunteers.
- Report any suspicious activity to your Internet service provider, as well as to your local cybercrime department of the police.
- Implement a policy for the disposal of IT equipment, media, & IT documentation.
- Use a paper-shredder for disposing of confidential HOW documentation.
- Screen telecoms or IT repairmen visiting the facility.

Section 13: HOW Event, Service, & Function Planning

The most critical time to protect a HOW is when there is a function, service, or event as these normally attract large crowds of people, members of the public, and the congregation. They are also normally advertised and mentioned on social media or in the press.

Depending on the size of the event planned, it may require weeks or even months or more of preparedness by the HOW security team.

Event, Service, & Function – Planning & Prevention

- **Event Controller:** Appoint an overall individual to be in charge of security and/or emergency management for the event, service, or function.
- **Resources Required:** It is critical that the HOW events planning team communicates details about the event to the HOW security to plan accordingly in terms of resources required. The event controller would in-turn need to ensure he/she arranges the appropriate combination of law enforcement, volunteer, and paid security manpower.
- **Risk & Threat Assessment:** Conduct an up-to-date assessment of the site both in terms of recent criminal or terrorist events, planned protests, or issues occurring in the neighbourhood.
- **Law Enforcement:** Communicate accordingly with local enforcement especially in regard to receiving any available intelligence; discussing possible traffic issues and/or road closures which may be required for the event; as well as possible requirements for explosive detection canines.
- **Intelligence & Briefing:** Ensure any intelligence regarding any threats to the event is shared as part of the briefing, as well as information on any VIPs or controversial individuals that may be attending the event.
- **System Site Check:** Ensure all security systems at the site are operational and tested. Also that the appropriate staff will be on duty to man this equipment for the event.
- **Personnel Equipment:** Check security personnel equipment such as 2-way radios, non-lethal weapons, medical equipment, and firearms (if applicable).
- **Operating Protocols:** Ensure the security team is aware of the various protocols for the event in terms of communication, searching, screening, patrolling, and what to do in the event of a security, fire, or medical emergency. Instructions should also be given to the team if a person needs to be denied entry or ejected from the event.
- **Parking Responsibility:** Parking arrangements should be pre-planned through the use of signage, road cones, traffic law enforcement, and possibly parking marshals. Ideally, the security team should not be focused on parking as this could divert attention from their role.
- **Deliveries, Event Staff, & Caterers:** The delivery of equipment and goods by individuals, companies, and organizations needs to be coordinated with the HOW event planner. Designated areas and time slots before or after the event should be planned for as to not disrupt security.
- **Shifts:** Plan shifts accordingly to ensure security manpower remains alert and their welfare needs are taken into account in terms of meals, drinks, the weather, and toilet breaks.
- **Medical Standby:** If medical personnel are to be available at the event, a suitable location would need to be provided, such as a first-aid station or a private area, to treat and/or stabilize medical patients before evacuation from the site.

- **Pre-Accreditation:** Some events may allow the pre-accreditation of individuals by issuing tickets, invitations, or photo credential ID cards. This process would need to be coordinated accordingly with the HOW security team. The security team members working the event would need to be made aware of the credential type to look out for and how to confirm it is correct.
- **Evacuation & Emergency:** Emergency evacuation would need to be planned accordingly for the event with a suitable evacuation site chosen to accommodate the individuals from the function.

Event, Service, & Function – Operational

These events would normally be divided into five distinct phases:

1. **Pre-Event**

    - A pre-event team arrives at a suitable period before the event, service, or function starts.
    - Roll call of security team and/or law enforcement present onsite.
    - Searching of outside and inside of facility.
    - Re-checking of personnel equipment, uniforms, & testing of communication equipment.
    - Re-checking of security systems (such as metal detectors, booms, etc.).
    - Re-checking of emergency equipment such as PA systems, loud hailers, firefighting equipment such as fire-reels and fire extinguishers.
    - Re-checking of medical equipment such as first-aid kits, AEDs, oxygen, stretchers, privacy screens, etc.
    - Reminding the security team they need to act within the parameters of local and national laws, and ideally, any serious situations need to be handled by law enforcement.
    - Discuss any executive protection that will be in place for VIPs.

2. **Ingress**

    - High volumes of pedestrian and vehicle traffic arriving at the facility.
    - Security bubble would be extended out.
    - Emphasis on monitoring and screening people and vehicles entering the site.
    - Would include the security team checking IDs, credentials, and invitations.

3. **The Function Itself**

    - Security-team focused on the facility and entry/exit points.
    - Investigate and/or question any suspicious individuals or vehicles around the HOW facility.
    - Monitor the inside of the facility for any disturbances or medical emergencies.

4. **Egress**

    - High volumes of pedestrian and vehicle traffic leaving the facility.
    - Security bubble would be extended out.
    - The security team needs to be motivated to keep alert.
    - Searching of the facility to ensure nobody has been ‘left’ behind, i.e., in toilets, etc.

5. **Debrief**

- This provides an opportunity to thank the HOW security team for its work and get any feedback regarding the success of the event, any issues, and lessons learnt.
- It also allows personnel equipment to be collected and returned to storage.

Section 14: Information Gathering & Agent Provocateurs

This could be by terrorists, individuals with psychological issues, or those with criminal intent.

Information Gathering – Planning & Prevention

- Most suspicious activities fall into the category of "common sense". HOW members should, therefore, be encouraged to share concerns that are self-evident.
- Some HOW communities may not have the budget/funding for full-time security personnel, therefore, the community and members themselves need to become force multipliers and become the eyes and ears of the community.
- Training programs must be carried out for the HOW security team to make members aware of what they need to look out for.
- Training items could include unknown individuals attending services, inappropriately dressed individuals (i.e., winter clothes in warm weather), people taking videos or photographs of the facility/site/member, and individuals having an unhealthy interest in the facility/community.
- Particular attention should be paid to individuals photographing children, asking about children's programs, or enquiring about the locations of classrooms.
- Part of the preparation work should include training for HOW security team members on how to approach such individuals in a friendly, non-hostile (intervention ready) manner. An advantage of this approach is that it provides a deterrent to the criminal showing them that the facility is well monitored. The HOW should always act within the parameters of the law.

Information Gathering – Operational

The plan would need to include protocols for dealing with suspected or actual information gathering:

- Taking photos of the suspects or using the facility's video surveillance system to record them.
- Writing down a vehicle number plate or making a note of the individual's description.
- Reporting it to the facility's appropriate person in charge of security so that law enforcement (local, national, or special police units) can be informed accordingly.
- Sharing of information with neighbouring communities and other houses of worship.
- Reporting to national organizations that monitor suspicious activity or hate crimes.
- Continuous ongoing community training, especially after events have occurred. However, care should be taken not to 'pigeon-hole' members into only looking for specific suspicious activities but rather an activity that is out of the ordinary.

With the commercialization of drone technology and advances in hi-definition cameras, UAVs have become a real threat in terms of information gathering by 'remote control.'

Some countries have laws regarding the use of drones operating in a non-line-of-site manner and especially in residential &/or commercial areas and, therefore, the sighting of a drone without any visible operator 'buzzing' your HOW facility may be suspicious and could therefore be reported to your local law enforcement.

Agent Provocateurs

Agent provocateurs, ‘first amendment auditors,’ free speech advocates, and social media live streamers are a very real potential threat to any HOW facility. They have been known to provoke security into acting against them. They can also potentially expose security weaknesses at a facility and, if handled incorrectly, create legal problems and/or negative publicity against the HOW targeted. Many of the same mitigation measures used for information gatherers can also be used with agent provocateurs.

At the same time, HOWs may be able to employ media monitoring (or regular web searches) relating to their HOW to identify whether their facility has come under criticism or undue attention. Because agent provocateurs often want to build a wide audience for their actions, HOWs may be able to learn of a potential incident long before it happens and plan mitigation measures accordingly.

Agent provocateurs can also be found on the scene of riots or demonstrations and could inflame tensions where a peaceful crowd becomes violent and acts against the HOW. Preparation is essential and should include legal rights & awareness training and protocols to deal with such individuals.

Section 15: The Enemy Within

Internal threats must NOT be ignored as these could be the greatest threat facing a house of worship. Some of these risks and threats should be identified when conducting the security survey of the facility and procedures and measures put in place to help mitigate some of the threat.

The Enemy Within – Planning & Prevention

- HOW organizations need to ensure that new or existing employees are appropriately vetted.
- Vetting may be difficult as many of these 'employees' are volunteers or lowly paid due to a lack of budget.
- Screening could include regular and ongoing credit checks, criminal checks, background checks, confirmation of address, pre-employment polygraphs, as well as previous employer reference checks. Checks of this nature should be in compliance with local laws which may vary widely.
- Employees need to complete a formal employment form which is kept on record by the organization.
- Have regular conversations on signs of potential vulnerability including gambling addictions or financial difficulties, marriage difficulties, pornography, drug use (legal, prescription, or illegal), etc.
- The organization should NOT ignore employee grievances, as well as domestic issues that could be affecting the individual (such as divorce, death in the family, economic issues, criminal or civil charges, etc.). Ensure these issues are identified, assessed, and revisited regularly.
- Given criminals may be interested in gaining access to insider information such as security measures, vulnerabilities, or operational details, be alert for signs of undue interest in times of services, cash collection, banking times, the number of security officers on duty, access points used, video surveillance camera coverage and blind spots, week physical perimeters, etc.

The Enemy Within – Operational

- All employees/volunteers should be screened by security on arrival at the site, especially regarding items being bought into the facility or being taken out.
- Document all material removed and returned from the facility.
- Offer counselling and medical support services to ensure employee openness in the event a vulnerability is identified (e.g., drug addiction), but be prepared to terminate employment if continued use/abuse constitutes an unacceptable risk to the HOW facility or members.
- Even if security awareness programs are in place for volunteers, employees, and the community, free knowledge of all security measures at the facility should be restricted to management and/or the facility's security team.
- Special care must be given towards the protection of children from abuse.

Section 16: Mail Handling & Deliveries

Even though the popularity of postal mail services has decreased, the use of delivery services, food deliveries, and courier services have become popular.

- Each HOW should have guidelines and/or a policy in place for the handling of letters and/or packages delivered by these types of services.
- A delivery/postal item could potentially house an explosive device or harmful substance such as a biological or chemical weapon.

Mail Handling - Planning & Prevention

- The HOW should create a clear written checklist in this regard.
- A dedicated area should be prepared for the handling/processing of these items.
- This could be an area separate from the main building or a dedicated ‘mail-room.
- Checklist items would include but are not limited to the following:
    - Verification that the package/delivery is expected by someone onsite.
    - An appropriate return address.
    - Awareness of package shape, size, and any strange smells, leaks, and/or discolouration emanating from the package/letter.
- If the budget allows, the facility should have a suitable x-ray scanner in place.
- Alternatively, if resources at the HOW are limited, a policy could be implemented to ban all deliveries/postal services directly to the HOW and rather make use of an external postal ‘box’. This would then allow the size of packages/letters to be limited and move the risk away from the HOW facility. The policy should include what to do in the event of the detection of a suspicious item and how to activate the necessary law enforcement response.

Section 17: HOW Facility Open/Close Policy

As part of the security and emergency plan, a HOW facility should have a procedure for opening and closing the site.

Facility Open/Close Policy – Planning

- A responsible person should be appointed for this function amongst either the community and/or one of the employees at the site.
- They should be assigned a unique set of keys, access credentials, or alarm codes. These should be specifically allocated to that person and not shared with others.
- The policy should be a basic simple-to-understand checklist that could typically be printed and mounted at an easy-to-see location such as inside the entrance door or at the alarm keypad.

Facility Open/Close Policy – Operational

Opening and closing a facility is a time at which the keyholder could be at risk of being attacked or robbed. Ideally, if the HOW facility has a contract with a security company, they should meet and greet the keyholder whenever the opening/closing occurs. This would also be helpful to protect those working late or opening the facility in winter when it is still dark.

Checklist – Closing	**Checklist – Opening**
Is the safe locked and valuables locked away?	*Any external signs of break-in or vandalism?*
Is the server room locked?	*Any new graffiti or a message left at the site?*
Has everyone left the building?	*Any internal signs of break-in or vandalism?*
Have the toilets been checked?	*Server room or safe found open?*
Is the oven off in the kitchen?	*Is there any environmental damage, water, etc.?*
Are all windows locked?	*Was the alarm on when you entered?*
Have you set the alarm?	*Any strange people loitering outside the facility?*
Are the facility's external lights working?	*Anything else out of the ordinary?*
Is the CCTV system operational?	*Other*

Section 18: Continuity of Operations (COOP)

The resumption of normal operation after an emergency is essential to the survival of the HOW.

Continuity for the Houses of Worship

- This planning would include how services will continue if the primary facility cannot be used, including back-up systems to retrieve important information. It would describe what activities must continue, even if the site is inaccessible (e.g., regular worship services) and what activities are not deemed essential (e.g., use of the site by external groups).
- The HOW could also consider establishing a formal "sister HOW" relationship with nearby congregations with reciprocal agreements for utilizing each other's facilities in the event of a disaster or emergency.
- Consider live streaming, podcasts, Facebook, or other social media options of ministry presentations when there has been a facility compromise preventing access.

Evacuation (and Re-entry)

- Planning should include how an evacuation will be conducted, including what form of alert/notification and where the primary assembly area(s) and secondary areas (if the primary location is inaccessible) are located.
- This would also include details of who will decide if the building can be re-entered and the process for determining this.
- Reunification/staging locations need to be identified and arrangement made to use these with neighbours, adjacent retailers, or other congregations.
- A simple checklist can be created for each room (laminated cards) on how to prepare in the event an emergency communication signal is broadcasted—locking of doors/windows; run, hide, fight (active attacker incidents).

Lockdown

- This planning would describe how the building(s), and areas within the building(s), will be secured to keep congregants safe from a threat (e.g., dangerous animal or intruder).
- It should include a site map and floor plan(s) of which doors to lock and which will need added security measures if lockdown/lockout occurs.
- Physical barriers and delays are essential in keeping the intruder/attacker away from the HOW congregation which is its main asset.

Shelter-in-Place

- How congregants will shelter at the location due to severe weather or other dangerous incidents outside the location (e.g., hazardous material incident), including what room/area should be used.
- Consider first any existing shelters, if nearby, where personnel can be transferred.
- Determine the number of personnel the shelter will hold.
- Assign shelter wardens to assist in preparation and management of shelter space.

Recovery

- Plan how the site will recover from an emergency event, including activities to support business operations (e.g., payroll), mental/emotional health (e.g., counsellors or debriefing for staff), and site operations (e.g., cleaning and refurbishment of buildings).
- Confirm (before it is needed) the HOW insurance coverage. Many ministries have “cancelled event” and other insurance coverage options that they may not be aware of.
- Consider how the clergy and HOW members would assist by visiting the sick and elderly, as well as providing financial, humanitarian, and social support to them after an emergency incident.
- Identify existing shelter areas within the organization—access to proper infrastructure (proper utilities, access to bathrooms, etc.).
- Plan signage or assigned procedures for directing personnel to the shelter area(s).
- Prepare food, water, supplies, clothing stocks storage, and distribution locations.
- Ensure the HOW communication officer liaises with the community, the media, and the necessary government bodies to provide additional support.

References

- Michael E. Knoke, CPP, *Physical Security Principles*
- David G. Patterson, CPP, *Implementing Physical Protection Systems: A Practical Guide, 1st Edition*
- ASIS International Guideline, *Facilities Physical Security*
- CAIR Best Practices for Mosque and Community Safety
- Jewish Federations of New Jersey Emergency Preparedness Guide
- All photos by Nathan Bearman and provided for use in this publication.

Useful Websites

- https://www.fema.gov/
- https://www.gov.uk/government/emergency-preparation-reponse-and-recovery
- https://www.cpni.gov.uk/security-planning
- https://cpr.heart.org/en
- https://www.fbi.gov/about/community-outreach

Disclaimer

This House of Worship (HoW), Security Response Plan is provided for informational and educational purposes only. It is intended to offer HoW guidance regarding good practices for protective security planning. Adherence to any recommendations included in this document will not ensure security in every situation. Furthermore, the recommendations contained in this document should not be interpreted as setting a standard of care, or be deemed inclusive of all proper methods of security nor exclusive of other methods of security reasonably directed to obtaining the same results. Use of this information is voluntary, and reliance on it should only be undertaken after an independent review of its accuracy, completeness, efficacy, and timeliness.

Please note that the best practices contained in the document do not constitute legal advice, should not be treated as such, and are not a replacement for legal advice.

Please check with legal counsel to ensure a full understanding of the legality of the best practices applicable to your HoW.

ASIS does not guarantee the accuracy, completeness, efficacy, or timeliness of such information. This document and its contents reflect the best available information at the time the document was prepared. Revisions to the recommendations in this document to reflect new data may be necessary.

ASIS does not warrant the accuracy or completeness of the document and assumes no responsibility for any injury or damage to persons or property arising out of or related to any use of this document or for any errors or omissions. All content is provided "as is."