ProtectUK

Evacuation, invacuation, lockdown, protected spaces

Original publication date
02/11/2020

1. Introduction

Requirement for guidance

Those with responsibility for Publicly Accessible Locations are advised to consider the threat from a broad range of terrorist methodologies. Such methodologies may include Vehicle as a Weapon, Marauding Attacks with either bladed weapons or firearms and improvised explosive devices etc. Planning your emergency response should such an incident occur would likely require a range of emergency responses, including a consideration of emergency evacuation, ‘invacuation’ (an inward evacuation) and lockdown procedures, alongside the use of protected spaces.

This document is intended to provide guidance for Publicly Accessible Locations in the planning and implementation of their site’s emergency response.

This document provides generic advice for all Publicly Accessible Locations: venues, buildings and events.

The responsibility for deciding your emergency response

The initial decision-making regarding the invoking of an emergency response is usually made by the management of the Publicly Accessible Locations. For outdoor festivals and other events, this may be the event/crowd safety manager in conjunction with the promoter/organiser. During an incident, initial decision-making should not be delayed pending instruction or action from the police. The speed of decision-making and implementation during an incident is critical.

Police will provide support, advice and guidance as soon as they are able, however this may not be immediate. In exceptional cases, the police may insist on evacuation, although they should always do so in consultation with the Security Manager or responsible individual. This must always be documented.

Actions taken by your site should be reasonable, necessary and proportionate, based upon the circumstances, particularly when they are necessary to protect life.

Requirement for planning

Publicly Accessible Locations should have an Emergency Response Plan, designed using the ‘deter,

detect, delay' principles. The aim of the plan is to minimise casualties (injuries and fatalities) in the event of an incident.

As a minimum, your emergency plan should include the following:

- Evacuation, invacuation and/or lockdown procedures and route assignments, such as floor plans, workplace maps, and protected/safe or refuge areas.
- Names, titles, departments, and telephone numbers of individuals both within and outside your company to contact for additional information or explanation of duties and responsibilities under the emergency plan.
- Identified personnel who will 'lead' in the evacuation to direct people to safe exits, e.g. marshals or wardens.
- Procedures for those employees who will remain on site to perform or shut down critical operations, or perform other essential services.
- First aid procedures and responsibilities.
- Procedures to account for all employees following an evacuation.
- The site of an alternative communications centre to be used in the event of an attack or incident wherever possible.
- A secure on/off-site location to store original or duplicate copies of accounting records, legal documents, your employees' emergency contact lists, and other essential records.
- A crisis response kit (grab bag).
- Consider instructing crowds to disperse upon evacuation. This reduces the risk of a secondary attack at a designated assembly point.

You may want to complete the Crisis Response Kit checklist

2. Response planning

When planning, it may be useful to consider your site's response in three phases:

1. Pre-incident (Thinking ahead)

2. Incident (Considering your options and taking action)

3. Post Incident (Recovery)

Pre-incident: thinking ahead

Developing a response plan

- make sure an individual (with a designated deputy or deputies) is responsible for the emergency response plan and its delivery
- it is important that your plan is co-ordinated and compatible with those of your neighbours, particularly if you rely on a shared space. You should also consider, once the capability is delivered, how this would be maintained/assured throughout its life
- anticipate potential threats and assess the risks
- develop response plans specifically for each site/location, possibly including individual buildings or spaces within the venue, and co-ordinate with neighbours

Ensure your infrastructure facilitates your plan

Ensure your infrastructure supports your procedures for an emergency response. This may include signage to identify specific emergency evacuation routes, the remote controlling and securing of entrance points and vehicle shutters, CCTV, alarms etc.

Prepare and train your personnel (staff, security, contractors and visitors where appropriate)

The key challenge for any site is the ability to be able to respond effectively to an incident, which will likely be confusing, evolving and potentially life-threatening. The regular and ongoing training and exercising in relation to different threat and attack scenarios will help prepare staff to effectively manage such situations; they need to be familiar with what is expected of them within their roles and what actions they need to take. Part of this training and preparedness should involve the effective

use of communications.

Please see CPNI's Marauding Terrorist Attacks guidance for further advice.

Make sure:

- your staff are aware of the threats (consider the ACT packages)
- there is a strong security culture across your organisation, including how to quickly and effectively report incidents
- you have ‘Standing Operating Procedures’ (SOPs) in place, and that they are regularly reflected and practiced within training exercises and briefings
- everyone understands their role and responsibilities
- staff are familiar with all evacuation routes (including outside buildings, sites, events or away from the Publicly Accessible Locations, protected spaces and assembly points). Some exercises should prohibit the use of one or more evacuation routes so that staff and contractors become familiar with alternatives
- where a site operates live/‘real time’ communication messages; e.g. making public address announcements, simulating a call to 999, radio communications under pressure etc., ensure regular training and exercising takes place.

You may want to complete the Crisis Response Kit checklist or visit CPNI's supplementary guidance – Announcements and Command and Control for more information.

Deny deter and detect hostile reconnaissance

- make sure staff remain vigilant, making the operating environment hostile for potential attackers
- demonstrate a strong security posture through visible and effective security activity. This will be enhanced through effective staff awareness, reporting processes, use of CCTV and deterrent communications
- make sure staff are appropriately trained and confident to manage any perceived hostile reconnaissance. This may include SCaN (See Check and Notify) Training

- make sure an effective procedure is in place to inform the appropriate authorities of any suspected hostile reconnaissance
- record the actions taken by your site

Read more about Hostile Reconnaissance.

Emergency response planning: Ten key actions

The below actions will assist your site in protecting people during an incident:

1. Have an incident response plan in place and implement it in the event of a terrorist incident. Train and exercise your plans regularly.
2. Have a communications system to confirm when an incident is taking place. Consider the relationship between your security team and centralised control room staff: the best picture is often from the ground. Report the incident to police immediately and alert people within the site/location. Do not wait for all the information before alerting the police.
3. Locate, track and monitor intruders/hostiles (e.g. via CCTV etc.) and communicate this to the police. They will require different information for different scenarios. The ETHANE model may help staff communicating with emergency services about what may be required.
4. You may want to complete the ETHANE checklist, which outlines the initial actions to take at a major terrorist Incident
5. Decide on the appropriate response of your site. Establish if the threat is external or internal. If it is within the venue, consider evacuation. If the threat or incident is outside, it may be safer to stay inside. Deciding upon and initiating evacuation, invacuation, lockdown and/or the use of protected spaces should be the responsibility of the lead individual. Have immediate access to key checklists for procedures and key information that needs to be recorded.
6. Instruct staff, visitors and contractors what they should do and where they should go. This direction could be directive or simply to leave the area by their nearest exit.
7. Reduce the number of potential causalities by deterring or where possible, preventing people entering the venue or site. Clear communications will be the most critical part of the delivery of this element.

8. Deal with the injured when it is safe to do so.
9. Remember to record and justify key actions and decisions taken.
10. Staff and visitors may have different responses to the same incident. Consider the impact of staff, contractors and/or visitors not following or directly contradicting instructions.

Consider both social media and press needs and have holding statements available. Where possible, actively monitor news channels, CCTV and social media channels

For further First Aid Guidance:

Go to CitizenAID

Go to St John's Ambulance

Go to the Red Cross

Delay the attack and protect your people

As the incident develops, consider:

- how your site could slow attackers. This may include causing them to waste time, energy, ammunition and weapons on overcoming barriers. Technology such as the deployment of 'Active Delay Systems' at specific locations may assist you. Such systems are designed to confuse, disorientate and slow the attacker(s). Your site's control of lifts, escalators and stairwell access may also help slow the attack's progress
- how your plans can maximise the opportunity for staff, visitors and responders to escape or stay safe
- how your plans can maximise the opportunity to protect your critical assets, e.g. your control room, air ventilation systems, servers or critical power sources

Go to the CPNI Active Access Delay Systems webpage or see CPNI's supplementary guidance - Physical barriers to delay and discourage attackers.

For further information, see below:

15.5 Appendix A: a summary of factors for consideration during an Incident for organisations

15.6 Appendix B: a summary of factors for consideration during an Incident for individuals

Post incident (Recovery)

Following an incident, your site will be looking towards the recovery phase and resuming normal operations.
Once it is formally confirmed there is no longer a threat, organisations can begin to engage in post-incident assessments and activities. Such activities may include:

- accounting for all staff, contractors and known visitors. This may be through direct contact with your staff, or via business continuity systems. This process will help you to determine whom, if anyone, is missing and / or potentially injured. It is important that HR records and contact details are regularly reviewed and updated for this purpose
- notifying the families of individuals affected by the incident, including the notification of any casualties
- making sure the early engagement of mental health professionals to which all staff should have access for appropriate psychological support. This should be accessible at the earliest opportunity. Remember those affected may extend beyond staff directly involved in the incident
- recording your site’s decision-making processes and actions
- making sure both press and social media statements are ready to go and are as accurate as possible
- identifying and filling any critical personnel or operational gaps left in the organisation as a result of the incident
- when appropriate, identifying ‘lessons learned’, incorporating them into training and exercising through a structured and documented debriefing process

3. Types of emergency response

There are a number of options for emergency response, including:

- full site evacuation
- phased evacuation (consider if you require dedicated searchers to remain)
- partial or zonal evacuation
- directional evacuation, in which staff, contractors and visitors are directed to specific exits and routes
- invacuation to safer areas, including protected space(s), if available
- partial invacuation
- no action required (a decision is made not to evacuate or invacuate)
- lockdown (this may be a partial or full lockdown)

Full site evacuation

A full site evacuation would be appropriate when directed by police and/or it is reasonable to assume the attack or threat is credible, and when evacuation will move people towards a ‘place of relative safety’. You may wish to direct people to ‘evacuate to their nearest exit’ and disperse, or direct them to specific exits.

It is important to note that the safety of particular routes may change during the course of an attack. For example, the use of lifts (in non-fire scenarios) may reduce evacuation times, but send people to an area where attackers may be located.

Directional evacuation

A directional evacuation may be beneficial if a specific area is, or is likely to become dangerous, or if an alternative route would result in people passing through or near to the area of threat. Selection of this strategy may increase the overall evacuation time, but could improve safety.

For this method of evacuation to work effectively, it would require staff and visitors to be familiar with the different routes and the names of the exits, which should be clearly labelled and communicated; e.g. Exit A, blue exit, floor 1.

Communication without alerting attackers is generally preferable, hence any use of code words either over public announcement systems or over radios would need to be included in your site’s planning, training and exercising.

For chemical biological and radiological incidents, consider evacuating uphill and upwind, staying away from the building heating and ventilation systems should the incident have occurred inside a building.

Phased evacuation and partial (zonal) evacuation

A phased and partial (zonal) evacuation may be appropriate in order to give priority to the people closest to, or most at risk from the threat. This approach is similar to a fire scenario, where typically the floor affected and two floors above are evacuated in advance of others. This allows for a controlled and prioritised evacuation, minimising the overloading of internal or external circulation routes. This method of evacuation may be particularly relevant for events and stadia where crowd numbers and densities may be high.

Invacuation including to protected space(s)

There are occasions when it may be safer to move people away from the threat while remaining inside the venue.

If the threat is outside your venue, or the location is unknown, people may be exposed to greater danger if the evacuation route takes them past the threat (such as a suspect device, contaminated environment or an ongoing external attack). Since glass and other fragments from IEDs may kill or injure at a considerable distance, moving staff inside Publicly Accessible Locations (including to protected spaces) is often safer than evacuating them onto the streets.

Invacuation requires pre-planning to help identify safer areas within your building. These locations should be identified within your emergency plans.

Protected spaces should be located:

- in areas surrounded by full-height masonry walls, e.g. internal corridors, toilet areas or conference rooms with doors opening inwards
- away from windows and external walls
- away from the area in between the building’s perimeter and the first line of supporting columns (known as the ‘perimeter structural bay’)
- away from stairwells or areas with access to lift shafts which open at ground level onto the street. This is because if compromised, blast could travel up them. However, if the stair and lift cores are entirely enclosed, they could make good protected spaces
- avoiding the ground floor or first floor if possible
- in an area with enough space to contain the occupants

When choosing a protected space, seek advice from a structural engineer with knowledge of explosive effects and do not neglect the need for air, toilet facilities, seating, drinking water, lighting and communications. Such provision would be necessary in order to accommodate people for an extended period (perhaps several hours or more).

Consider duplicating critical systems or assets in other buildings at a sufficient distance to be unaffected in the event of an emergency, which would deny you access to you own. If this is not possible, try to locate vital systems within a part of your building which offers similar protection to that provided by a protected space.

Any invacuation will need to be supported by a communication giving clear and concise instructions. When crafting communications, consider both the effectiveness on staff but also how this may be received (and acted upon) by attackers. The crafting of such messages requires considerable thought and practice in delivery.

Go to the CPNI Protected spaces webpage.

Dynamic lockdown

Due to the wide variety of Publicly Accessible Locations across the UK, it is not possible to give prescriptive advice on whether or how to lockdown sites or events in response to a fast-moving incident such as a firearms or weapons attack. This guidance however aims to provide planning considerations applicable to most sites.

If preventing an attack has not been possible, the ability to frustrate and delay the attacker(s) and reduce the number of potential casualties may be greatly increased through the application of dynamic lockdown.

Advance planning and flexibility within those plans is required. In order to achieve dynamic lockdown, planning should:

- identify all access and egress points within both the public and private areas of the site. Access points may be more than just doors and gates
- identify how to quickly and physically secure access/egress points. Consider both the design of the locking device at these points and whose role it would be to secure them

- identify how lockdown can be quickly reversed should the need arise (such as in the event of fire)
- identify how to disable lifts without returning them to the ground floor
- identify how to stop people leaving or entering the site, and direct people away from danger
- identify how your site can be zoned to allow specific areas to be locked down
- include staff roles and responsibilities and train staff in these
- processes need to be flexible enough to cope with and complement evacuation, invacuation and movement to protected spaces

Dynamic lockdown, especially during the ingress phase of an event, may lead to people being ‘locked outside’ and more vulnerable to the perceived threat. However, allowing continuing ingress may permit the threat to enter the venue and make those inside more vulnerable. Each case must be assessed on the information known at the time; good internal and external information and communications systems are crucial. This decision-making process should be considered in staff training and exercising.

Refer to Marauding Terrorist Attacks:

Lockdown guidance and animation, testing and Exercising guidance

The decision not to evacuate or invacuate

A decision not to evacuate or invacuate would be reasonable and proportionate if, after evaluation by the responsible person, the threat is deemed implausible (e.g. a hoax). In such circumstances, police may provide additional advice and guidance relating to other risk management options. It may be considered desirable to ask staff familiar with the venue to check their immediate surroundings to identify anything out of place, making them aware of what to look for including hostile reconnaissance.

Do not disregard the possibility that the ‘hoax’ may have been a test of your site’s processes and part of a hostile reconnaissance operation.

Read more about Search Planning.

4. Other Considerations

Population of Publicly Accessible Locations

When considering your site, it may be beneficial when developing your plans, to understand how the crowd, its density, distribution and demographic may change at different times. This in turn may influence how you best manage the co-ordination of any evacuation or invacuation.

Suitability and performance of exit routes

The suitability (e.g. with regards to trip hazards, lighting, pinch-points etc.) and capacities of evacuation routes and exits should be regularly assessed. Knowing the limitations of a particular route or exit is helpful in decision-making in order to determine how quickly your crowds can safety exit.

Evacuation procedures should also put adequate steps in place to ensure no one else can enter the area once an evacuation has been initiated.

Evacuation in non-fire scenarios is not the same as evacuation due to fire

Buildings and events, but not all Publicly Accessible Locations, must be designed, maintained and operated to reduce the risk to safety arising from fire. Consequently, staff, contractors and visitors are likely to be familiar with the principles and practice of fire drills including evacuation.

In some emergency scenarios such as a terrorist attack, the appropriate response may be not to evacuate. Where evacuation may be required, the evacuation response may differ to that of a fire. For example, people may be directed to specific exits or to avoid a particular route or area.

For this reason, it is suggested the activation of the fire alarm to initiate evacuation should be avoided to reduce the possibility of an incorrect response. Public Address (Tannoy) systems, if available, may provide more flexibility to provide information and instructions appropriate to the scenario and to provide positive confirmation to staff and visitors that the emergency is real. This will help to reduce any potential delay in response.

Risks arising from movement in Publicly Accessible Locations

The sudden movement of large numbers of people creates its own risks. This movement may arise from the fear of a terrorist attack as well as an actual threat. People may be frightened and the surrounding crowd may move in conflicting directions and/or in a rapid or disorderly fashion. Disorderly movement may also increase the risk to those more vulnerable such as children, elderly, or people with impairments.

In high crowd densities where there is rapid or disorderly movement, people are more likely to experience a slip, trip or fall, which may in turn lead to trampling or crowd crush, or they may move into hazardous areas such as roads or platform edges. These risks may be exacerbated by poor footway conditions, stairs and escalators. Where stairs are intended to service high crowd flows (such as at stadiums), the stairs are designed with handrails to separate stair channels and with head-of-stair barriers. Some public places which feature occasional high-density crowds do not always have these safety features.

Personalised emergency evacuation plans

Under current fire safety legislation, the person(s) with responsibility for the building is required to provide a fire safety risk assessment, including an emergency evacuation plan, for all people likely to be in the premises, including those with disabilities. The emergency evacuation plan should include details of how it would be implemented.

The Government guidance on Fire Safety Risk Assessment: ‘Means of escape for disabled people’, provides detailed guidance on how to plan effectively to respond to a fire.

It is sensible to develop personalised plans for staff and visitors with disabilities in the event of a non-fire emergency requiring evacuation, invacuation or movement to a protected space. Designate those responsible to assist them as appropriate.

Go to the Government Guidance on Fire Safety Risk Assessment: Means of Escape for Disabled People.

Control room response

The actions control room staff are able to take, in some incidents, may be limited. Their ability to support public safety will be affected by:

- the degree to which they themselves are at risk
- their own knowledge of the full nature and extent of the incident
- communication channels available
- their familiarity with appropriate response options
- the speed at which they are able to recognise, accept and respond to the incident
- how psychologically able and prepared they are to respond correctly

Regular training and exercising will help to reduce some of these limitations, allowing for a more effective and efficient response to an incident.

Consider having alternative off site control room arrangements, should a contingency be required. This may be achieved by having a mutual agreement with nearby premises where an emergency

control can be established at short notice. The contents of a Crisis Management Kit ‘Grab bag’ could also be stored here.

See CPNI's Incident Response & Command & Control page for more information.

Communications

Alerting staff and visitors

Your emergency response plan must include a way to alert staff and visitors, including those with impairments that an incident is occurring. The alert may be a direction to evacuate, or other actions to take to help keep them safe.

Public Address (PA) Systems: consider the use of code words for different incidents, dedicated tones or pre-recorded messages to instruct a particular emergency response. Should your site use code words, remember they will only be understood by a specific audience and may therefore be limiting in

certain situations. The response to such code words will also require regular training and practice. Note the use of a PA system will require a power source.

Internal messaging systems: hand held radio communications are often the most effective during a fast-moving incident such as an marauding attack, however text, email, staff phones, staff alerts/pagers, generic group messaging, such as WhatsApp, or ‘Pop ups’ on employees’ computers may be sufficient for slow moving incidents or during the recovery phase.

- the use of Variable Message Signs (VMS) at events or in public spaces
- a dedicated ‘lockdown’ alarm tone
- word of mouth

At some stage, an ‘all clear’ message may be required.

Managers may also wish to consider the following steps:

- make sure alarms are distinctive and recognised by all staff as a signal to evacuate the work area or perform responses as identified in the plan
- stipulate that alarms must be heard, seen, or otherwise perceived by everyone in the workplace. Use tactile devices to alert employees who would not otherwise be able to recognise an audible or visual alarm
- consider providing an auxiliary power supply to ensure continuity of your security systems
- hold an accessible and regularly updated list of key personnel such as the security manager, first aid staff, managers etc. (in order of priority), to notify in the event of an emergency
- if used, train your staff in the use of code words. Be aware that the frequent use of code words in public areas (e.g. railway stations) are soon recognised by regular users of those spaces (e.g. commuters) and may trigger responses from them
- for multi-occupancy sites, methods of communication from site managers and between all businesses need to be considered

Informing and updating emergency services

Communication with the emergency services prior to and during the incident is critical. Communication systems should be regularly tested.

Media and Communications

Avoid revealing details about specific incidents to the media or through social media without prior consultation with police. Do not provide details of threats or incidents or the decision-making process relating to emergency response.

For further information, Go to the CPNI Website: Crisis Management for Terrorist Related Events

5. Appendix A: Emergency response planning – organisations

Plan – pre-incident

The following list provides a guide to elements your organisation/site could consider. There will always be a degree of variation and relevance depending on the nature of the event, location, weather and other impacting factors.

Consider threats, vulnerabilities and assess the risks

- develop a plan (Emergency response plan)
- security manager to plan for evacuation or invacuation, identify protected spaces
- identify individual's roles and responsibilities (e.g. security manager, personal evacuation plans for disabled people etc)
- provide relevant guidance and information to staff, contractors and visitors
- prepare your personnel and contractors through training and exercising
- identify critical operations and functions
- develop pre-scripted messaging/alerts as to how you will communicate with staff, visitors etc

- plan how you will deny, detect and deter hostile reconnaissance

- plan how you will deny, detect, deter and delay attacks or threats to protect your most valuable assets (physical and personnel measures)

- ensure infrastructure: signage, lighting, floor levels, lifts, stairs are clearly marked and labelled. Ensure CCTV is functional in order to facilitate an evacuation/invacuation

- prepare floor plans

- establish if your control room is capable of being operationally effective against different attack types and whether it can be appropriately secured/defended

- regularly check systems and equipment

- prepare crisis response kits (incl. personal information about your employees)

- establish working relationships with neighbours

- prepare checklists to support emergency responders

- make sure staff have adequate and up to date first aid training

Remember: Plans must be event and location specific

Incident – evaluate

Consider your options and use your judgement.

- stay calm
- gather information
- assess the situation, determine the type of incident, location(s), attackers, hazards, weapon(s). Do not wait for police

- implement plans
- establish where is the safest place, or if any response is required. Is it safe to evacuate? Are there other attackers, devices, obstructions, fires etc?
- establish the safest route(s) to leave
- consider: full site evacuation, staged/zonal/partial/directional evacuation or invacuation, internal/inward invacuation to protected space/area, lockdown, decision to take no response
- do any critical operations require protecting or shutting down?
- can I stop other people entering the site?
- determine if a search of the site is required
- monitor news and media channels
- communicate with partners

There is a danger you may be overwhelmed with information. Determine how to gather and transfer information in a controlled manner to support an effective response.

Incident – respond

Take responsibility

Leadership is key. Complete a dynamic risk assessment and take action:

1. communicate: let staff and people know what is happening and where possible, advise the most appropriate response. Keep personnel updated
2. call 999 – Follow the RUN HIDE TELL principles if appropriate
3. make contact with the emergency services and ensure they are updated appropriately
4. continue to monitor the progress of attackers using your technological assets e.g. CCTV
5. prevent people from entering the venue if it is not safe to do so

If lockdown is implemented, manage lockdown during the course of the incident. You may need to reverse lockdown in the event that the secure area has been breached or a fire has started/poses a significant hazard.

Post incident recovery

1. account for all individuals
2. determine a method for notifying families of individuals affected
3. make sure professional psychological support for all staff affected at the earliest opportunity
4. consider processes for a further emergency response in the event the incident expands
5. record your responses
6. determine if a search of the site is required
7. identify and fill critical personnel and organisational gaps
8. use lessons learned to train and rehearse staff

Read more about Business Continuity

6. Appendix B: Individuals – Personal safety

Plan – pre-incident

Think ahead:

- what are your plans if there were an incident?
- be aware of your surroundings including evacuation routes (events and building)
- note the locations of exits
- identify areas where you could take cover (hide/cover from view)
- make sure you have contact details of important individuals e.g. family

- understand what to do for building alarms
- consider sometimes using different entrances into work so you are more familiar with alternatives for evacuation

Incident – evaluate

Consider your options:

1. stay calm
2. assess the situation as quickly as possible
3. where possible identify where you are in relation to the incident
4. establish where is the safest place
5. listen to instruction communicated by those in authority
6. your options will be:

- evacuate and get yourself and others to safety, possibly via safe routes. RUN
- remain where you are and await further information
- go to a protected area/shelter
- HIDE

Incident – respond

Take responsibility

Leadership is key: make a dynamic risk assessment and respond:

1. evacuate in a safe and orderly manner where possible
2. identify the safest route

3. assist others if it is safe to do so
4. go to RVP/disperse as appropriate
5. TELL police when it is safe to do so

Post incident

Recovery

1. If you have witnessed the attack, report what you saw. Make yourself known to police. Any photographs or video footage should be passed on to the police
2. If you are a victim of an attack, contact the police
3. Contact family and friends to let them know you are safe

Remember: Follow the RUN HIDE TELL principles

Managing risk

- have you conducted a risk assessment?
- has an individual been appointed who is responsible for security?
- have you an Emergency Response Plan?
- under what circumstances would you instigate an evacuation/invacuation/lockdown?
- have you established the safest evacuation routes and protected spaces?

Physical security factors

Critical points

- are there critical areas of the site that need to be shut down or are vulnerable?
- can you lockdown the site?

Crowd density and building occupancy

- can the entrances, exits, routes and protected spaces accommodate the expected evacuation capacity?
- are your exits ever inadvertently blocked e.g. during loading or unloading?
- can you prevent people entering?

Factors that affect the suitability of egress routes may include:

- stairs/escalators
- lifts
- exits (preferably opening outwards)
- seating and gangways
- signage to identify exits and routes
- widths and capacities/pinch points and obstructions/distances/slip/trip/fall
- evacuation timeframes
- volume of staff/visitors
- have you identified obstructions to an evacuation or invacuation route?

Building structure

- Have you identified what risks or protection the building structure offers against different attack types, for example, glazing, steel frame, brick work?

Access control

- Will your access control measures prevent escape or protect staff?

Lighting

- Is this suitable to support an invacuation or evacuation?

Control rooms

- Are they protected from different attack types?

Alarms

- Do you have alarms to alert your staff and the public?

CCTV

- What does it cover, is it monitored and can it track an attack?

Hazards

- Have you removed items and hazards that may assist a terrorist attack? (fuel, scaffolding

poles etc.)

Read more about Good Housekeeping.

Electrical supply

- Do you require backup generators?
- Is the electricity supply protected?

Personnel security factors

Threat awareness

- Have staff been briefed on threats and methodologies?

Training and rehearsal exercising

- have you conducted rehearsal exercises to validate learning?
- when did you last rehearse?
- when did you last train your staff? e.g. first aid, evacuation
- do staff know your protected places, routes and exits?
- can staff recognise suspicious behaviour?
- can staff respond effectively to suspicious items?

Role and Responsibilities

- do staff understand their roles and responsibilities?
- what are the roles of coordinators and evacuation marshals during an incident?
- have you identified what equipment you should provide In the event of an incident?
- do you have plans for safely evacuating/invacuating vulnerable and disabled staff and visitors?

Communication

Are communication networks effective?

Alerts and messaging

- what alerts, alarms, coded and/or pre-scripted messaging have you prepared?
- how do you alert employees and visitors to an incident?

Command and Control

- how will you communicate: radio, PA/VA, mobile phone, social media?
- are you able to contact other sites and partners?
- can you stop others entering?
- who will inform the emergency services?
- can staff communicate directly with and assist the emergency services?
- have you a media strategy?

Recovery

- have you a Business Continuity Plan?
- how do you account for employees after an evacuation?
- do you know who your critical staff are?

7. Appendix C: ETHANE - Initial actions at a terrorist major incident

Exact Location

- confirm nearest junction or exact address
- geographic size of the incident

Type of Incident

- explosion, building collapse, firearms incident etc.

Hazards

- identify the hazards present or suspected (such as number of attackers, types of weapons etc)
- consider potential or secondary devices

- is evacuation or invacuation necessary and safe?

Access Routes

- update with routes that are safe to use by the emergency services
- clarify routes which are blocked
- nominate and search the RVP

Number of Casualties

- list type and severity
- approximate number of dead, injured, survivors and witnesses

Emergency Services

- list those services present and those required
- conduct a joint dynamic hazard assessment with the emergency services

KEYWORDS
EVACUATION
INCIDENT MANAGEMENT
EMERGENCY SERVICES
RESPONSE
PUBLICLY ACCESSIBLE PLACES
PALS GUIDANCE
PALS
PUBLICLY ACCESSIBLE LOCATIONS