

The Principles of Working as a Security Officer in the Private Security Industry (Refresher) Self-study course book



Name

Learner N°:

Training Provider:

Start Date:

End Date:

All rights reserved. No part of this product may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, including electronic, photocopying, recording or otherwise, without the prior permission of Highfield Products Ltd. This includes the sharing or uploading of whole or partial copies online or on social media, whether on personal or business accounts.

Any unauthorised act may result in civil or criminal actions.

The publisher of this book has made every effort to ensure the accuracy of the information contained in this book. Neither the author, Highfield Products Limited nor anyone involved in the creation of this publication accepts responsibility for any inaccuracies or failure to implement correctly, however caused.

Disclaimer of Endorsement

Reference to or any image of any specific commercial or non-commercial product, process or service by company name, trade name, trade mark, service mark, manufacturer or otherwise does not constitute or imply endorsement or recommendation by Highfield Products Limited.



Highfield

Introduction

The Principles of Working as a Security Officer in the Private Security Industry (Refresher) self-study coursebook and workbook has been written to support the delivery of 3 self-study learning outcomes from 'Unit 1: Principles of Working as a Security Officer in the Private Security Industry (Refresher)'.

To undertake the learning you will need a minimum of **4 hours** to read the content and demonstrate your understanding of each learning outcome in the workbook provided. If the workbook is being used as self-study before attending face-to-face training/assessment, it must be returned to your training provider before you attend.

The learning outcomes are listed below with a recommendation of how many hours you are to allocate to each piece of learning.

Learning outcome	Content	Recommended hours of self-study
1	Know how to conduct effective search procedures	30 minutes
2	Understand how to keep vulnerable people safe	1 hour 50 minutes
3	Understand terror threats and the role of the security operative in the event of a threat	1 hour 40 minutes

Important note: this course book is only to be used by delegates who have purchased or have been given an individual copy (to keep) of the Highfield book as part of their course.

The Principles of Working as a Security Officer in the the Private Security Industry (Refresher)

Contents

Introduction	2	Learning outcome 3: Understand terror threats and the role of the security operative in the event of a threat	
Contents	3		
Learning outcome 1: Know how to conduct effective search procedures			
Rights to search	4	Terrorism	12
Types of search	4	Threat levels	12
Searching people	4	Common terror attack methods	13
Employees and search clauses	4	Actions to take	13
Searching other visitors	5	Suspicious packages	14
Searching people and their property	5	Suspicious activity	15
Equipment for conducting searches	5	Responding to suspicious behaviour	16
Searching safely	5	See it. Say it. Sorted.	16
Precautions to take	6		
Actions to take if a search is refused	6	Appendix 1	17
Searching vehicles	7		
Searching rooms or buildings	7		
Search documentation	8		
Dealing with property found during a search	8		
Restricted/prohibited	8		
Illegal items	9		
Actions to take if an incident or an accident occurs during searching	9		
Learning outcome 2: Understand how to keep vulnerable people safe			
Duty of care for vulnerable people	10		
Vulnerable people	10		
Drink/drugs	10		
Alone or receiving unwanted attention	10		
Potential victim of domestic violence	10		
Young people	10		
Indicators of child sexual exploitation	10		
Actions towards vulnerable people	10		
Sexual predators	11		
Indicators of abuse	11		
Allegations of sexual assault	11		
Anti-social behaviour	11		

Throughout this publication there are references to country specific content. These references are highlighted by the use of the following icons:



Learning outcome 1: Know how to conduct effective search procedures

Rights to search

Security officers, as private members of the public, have no legal or statutory right to search any person, vehicle or building without permission.

Under no circumstances can you forcibly search someone.

It is most important, therefore, that you actually obtain permission from a person you wish to search (beforehand). Searching someone without the necessary consent could result in:

- criminal proceedings for assault being taken against you
- civil action (compensation) being taken out against yourself and/or the security company
- a criminal case against a person committing a crime failing, because the search that found the evidence was illegal as consent was not obtained

Types of search

The types of searches you use will be dependent on the type of site, the people on it, the property involved and the client's policies on searching staff and visitors.

What you are required to do as a security officer will be specified in the site's A.I.s. You must follow these guidelines at all times. Subject to your site's search policy, you may be required, for example, to search:

- people (and/or their bags)
- vehicles
- property (rooms, buildings or intellectual property)

Searches can be:

- general - when everyone is searched
- random - when a random selection of people are searched (e.g. search every fourth person)
- specific - when specific individuals or vehicles are searched for specific reasons (suspicious people, vehicles/packages etc.)

Searching people

People may need to be searched before entering a site as a condition of entry or before leaving it and as part of the site admission policy.

They might require searching to stop them from bringing any weapons, drugs, suspect packages or other unauthorised items onto the site or they may need searching before they leave to ensure that they are not accidentally or deliberately taking away any of the client's property with them.

Employees and search clauses

Some client companies have specific clauses in their employees' contracts of employment requiring them to consent to a search at any time when requested to do so by a member of either the security team or the senior management. Such clauses are intended to reduce incidents of employees stealing goods or property from the client. These clauses usually explain that employees refusing a reasonable search request would be in breach of their contract of employment and therefore liable to disciplinary proceedings or even dismissal.

Information about such clauses, as well as details on whom, how often and how security officers are required to search employees will be found in the site's A.I.s.

Even where such clauses are in operation on a site, you must still seek permission before a search can be carried out - you still cannot search any person against their will.

Learning outcome 1: Know how to conduct effective search procedures

Searching other visitors

As a security officer, you may also be required to search staff, visitors or customers to a site prior to allowing them entry. Again, permission must be obtained before a search can take place. Anyone refusing to be searched should be either refused entry or the matter should be reported to the person they are trying to visit.

If a site has a 'point of entry' search policy, this should be clearly displayed at the entrance to explain the requirements to potential visitors.

You have no other specific powers to deal with people who refuse to be searched. If, however, you have reason to suspect that a person leaving a site (or someone having been refused entry for refusing to be searched) is in possession of either stolen property or an offensive weapon, then you should note the person's description, watch to see which direction they go in and report the matter to your supervisor or manager.

Searching people and their property

Searches should be conducted in a friendly, routine way so as to reduce any feelings of embarrassment that the person might feel. They must not be seen as an act of discrimination or by way of a particular security officer being obstructive.

All searches should be carried out in a polite and courteous manner. Some people may feel intimidated or worried when being searched, while others may be used to it. You should talk to people as you search them to help make them feel at ease. You should also try to carry out the search as quickly and as efficiently as possible, thanking them for their assistance afterwards.

Equipment for conducting searches

It is important that you know and understand the correct procedures when using the different types of search equipment. Equipment could include:

- handheld metal detectors (e.g. search wands - ensure that you know the sensitivity of the equipment)
- archway metal detectors (you should know the calibration settings)

- baggage/packages X-ray scanning, tray for smaller belongings
- search mirrors with lights
- gloves
- torches
- search dogs (trained to detect specific threats of concern)

Searching safely

It is always important to fully explain the search policy.

For your own safety, you should only search someone of the same sex as yourself. The SIA has published guidance for door supervisors on searching transgender individuals www.sia.homeoffice.gov.uk/documents/sia-ds-trans-guide.pdf

However, you must still follow your company A.I.s.

This is to prevent any malicious allegations being made that you have indecently assaulted the person while effecting a search.

There is nothing wrong with a male security officer asking a female to empty the contents of her handbag and pockets onto a table so that her property can be checked, (often called self-searching) but he should not 'pat her down' or otherwise touch her to detect unauthorised items. Self-searching also minimises the risk for contact with infectious diseases; should you not feel comfortable placing your hands onto an individual this method is a viable alternative. Many sites that carry out regular searches now employ security officers of both sexes for this very reason. Self-searching is also recommended for children and young people to avoid touching the individual.

Remember, the permission from the parent/guardian is needed to search a child or young person. The cooperation of the parent/guardian can help reduce any anxiety that the child or young person maybe feeling.



Learning outcome 1: Know how to conduct effective search procedures

NI

In Northern Ireland, discrimination is illegal under the following laws:

- The Race Relations (Northern Ireland) Order 1997
- The Sex Discrimination (Northern Ireland) Order 1976
- The Disability Discrimination (Northern Ireland) Order 2006

As a security operative, you cannot refuse entry or evict anyone on the grounds of sex, race, colour, disability or physical appearance. Should you refuse entry to or evict an individual for any of these reasons alone then you will be committing an offence. The individual who has been discriminated against has the right to make a formal complaint to the premises management requesting an apology, a commitment that such discrimination does not reoccur or even compensation. If the issue is not dealt with to their satisfaction, they may even take legal action against you and your employer.

Precautions to take

To prevent any false allegations of theft being made against you, you should always try to have another security officer or member of staff present during a search to act as a witness. Also, another officer is always an advantage in case of violence. It is also advisable to carry out the search in an area covered by CCTV.

Also, when the emphasis on the searching is for weapons, you may wish to use the slash-proof gloves as protection against knife injuries or use handheld metal detectors (search wands) that can indicate the presence of both knives and firearms.

If it is feasible to do so, have an empty table in a designated search area with good lighting so that you can ask people to put the contents of their pockets and bags on to it for inspection prior to the outer clothing being searched.

Although all members of staff and the public need to be treated with respect and consideration during a search, particular care should be taken when dealing with people with physical or learning difficulties, children and young people, and the protected characteristics identified in the Equality Act 2010 and the laws relating to discrimination in Northern Ireland (see module 1, chapter 2):

- age
- disability
- gender reassignment
- marriage and civil partnership
- pregnancy and maternity
- race
- religion or belief
- sex/gender
- sexual orientation

When carrying out searches of a person, especially children and young people, 2 staff members should be present during the search. The individual should not be asked to remove clothing other than outer garments like coats.

Hazards when searching could include:

- drugs coming into contact with skin
- needles/sharp objects
- infectious diseases
- weapons
- violence
- malicious allegations
- uncooperative visitor/client/customer

Body searches need to be made in a thorough and systematic way in order to ensure that nothing is missed. You should devise your own method of searching and should use the same system every time so that you do not forget to search particular areas.

A good way to search is to start at the front at the top and to work your way downwards, then change position to behind the subject to repeat the process.

Actions to take if a search is refused

Some people do not like being touched by anyone they do not know. A refusal of a search does not always indicate an illegal act. All people should be considered innocent unless there is evidence to indicate potential guilt.

The reason for the search must be explained to each individual. Visitors need to be aware it is a condition of entry and staff should be aware that it is a condition of their employment.

If a visitor refuses a search, they should be denied entry and the person that they were due to visit should be informed.

If a member of staff refuses a search, they should also be refused entry and their line manager informed.

The site A.I.s should detail what actions to take if a search is refused upon exit. The A.I.s will also state how a search should be recorded. All searches must be recorded, this may be on a search register or other report, or CCTV.

Learning outcome 1: Know how to conduct effective search procedures

Searching vehicles

The same rules apply with vehicles. Searches may be requested at the point of entry, on exit or may be a part of employee search clauses. Permission must still be sought prior to conducting the search of any vehicles driven by a member of staff or a visitor to the site.

Some sites require vehicles to be searched, including cycles, motorcycles, cars, vans and possibly heavy goods vehicles. You must, as in all cases, follow your company assignment instructions, however there are some basic steps that you can follow to ensure your own and others' safety:

- ensure that you use the appropriate PPE, including high-visibility clothing and safety footwear
- avoid inhaling vehicle fumes
- be aware of other motorists
- constantly monitor for hazards and risks in the search areas
- ensure engine is off and keys are controlled, i.e. not with the driver
- ensure the vehicle is parked in a safe designated location with the parking brake applied
- ensure the driver and any passengers are visible and in a safe location
- ensure that search locations have good lighting, CCTV and a witness where possible



Areas that you may be required to search include:

- under carpets, seats and door pockets
- engine compartment including hidden areas such as behind the battery
- wheel arches
- underneath the boot, including toolbox and spare tyre compartments
- any manufacturer-made or adapted voids
- cargo areas of vans and heavy goods vehicles



The level of search will depend upon the level of risk and therefore security on the site you are working at. All searches must be systematic to ensure all areas are searched thoroughly.

Searching rooms or buildings

Outdoor areas, buildings or individual rooms may need to be searched. This is often a requirement of the pre-entry checks to ensure that a premise is safe to open to staff and possibly the public. The pre-entry check is a systematic method of looking for any potential health and safety hazards. During your shift, you may also be asked to search for specific items/people such as:

- drugs
- weapons
- suspicious or missing people
- criminal activity
- suspect vehicles
- suspect packages
- signs of intrusion
- stolen, lost or damaged property

Learning outcome 1: Know how to conduct effective search procedures

Similarly, you may be asked to carry out searches as part of the company lockdown procedure. This may involve checking all rooms to ensure lights and equipment, such as portable fires or fans, have been switched off, toilet areas to ensure no one has hidden/stowed away, collapsed or fallen asleep in them and checking that all doors and windows are closed and locked if required.

Before conducting any search, you must ensure that you have sufficient support from colleagues to be able to conduct the search efficiently, effectively and safely. You will also need to ensure that you have any necessary equipment with you to assist in the search, and that you have a suitable method of calling for assistance if necessary.



Search documentation

Sites that require the security team to search people, their property or vehicles must provide a suitable method of recording searches. Accurate search records help to:

- ensure and show that search policies are being complied with
- protect security staff and the person being searched against malicious allegations
- act as evidence in criminal/disciplinary proceedings to prove a lawful search took place

Most sites or companies will provide security staff with a formal search register or book to record details of searches conducted on the site. Some sites require search details to be recorded in an incident report form.

Search records are to be completed by the security officer(s) conducting the search, and should contain details such as:

- day, date and time(s) of search
- location of search
- details of person searched
- details of vehicle/driver searched
- details of searching officer (and any witnesses)
- reason for search
- details of search refusal
- details of anything found during search
- any action taken
- signature(s)

Dealing with property found during a search

Any stolen, illegal, suspect or unauthorised items found must be dealt with correctly, following the site's AIs. The control room or a supervisor should also be informed.

Possible actions, depending on what is found and under what circumstances. The item may be restricted, prohibited or illegal.

Restricted/prohibited

The item is against the company policy. As a security officer, you should provide a verbal explanation or warning. The item may be returned to a vehicle or retained by security. Entrance can be granted and the item returned upon exit.



ALWAYS follow the procedures specified in the site's AIs.

Learning outcome 1: Know how to conduct effective search procedures

Illegal items

Illegal items found during a search will, in most cases, lead to the refusal of entry or potentially removal from site. In all cases, you must report to your control room or possibly senior management for advice. Upon their instructions, you may seize the item and refuse entry or escort the person from the premises or you may seize the item, arrest the person and call the police. In the latter case, you will hand the item and the person over to the police. In the case of the individual being an employee, you or control may need to contact the HR department. In all cases, you must record the incident as per the site A.I.s.

Actions to take if an incident or an accident occurs during searching

Occasionally, something may go wrong during a search of a person or vehicle. This could be a medical emergency, e.g. heart attack or a collision with another vehicle. In these rare occasions you may need to:

- follow your A.I.s
- call an emergency service
- summon the first-aider
- cordon off the area

In all cases, you will need to complete your notebook/incident report in addition to other documentation such as a search log.



Learning outcome 2: Understand how to keep vulnerable people safe

Duty of care for vulnerable people

As you go about your daily duties as a security operative, you will come across and have to deal with a whole range of people, be they customers of the premises or members of the public. Anyone who comes into the premises you work at may be or become vulnerable while you are carrying out your duties, so it is important to understand that you have a duty of care to them.

Duty of care: a moral or legal obligation to ensure the health, safety and welfare of others.

People may not always appear to be vulnerable, as a security operative it is best practice to ensure a duty of care for everyone.

Vulnerable people

As part of customer service and your role in protecting people from harm, you need to be aware of any people who may fall under the category of vulnerable people (people who may be at risk from harm). The following are factors that may put a person at more risk than others:

Drink/drugs

- Reduced inhibitions and the appearance of being over-friendly
- Uncoordinated movement increasing the risk of them hurting themselves
- Displays of aggression
- A change in perception of their own abilities and limitations
- Decreased ability to make informed decisions

Alone or receiving unwanted attention

- Apparently separated from friends and looking distressed
- Receiving apparently unwanted attention from others
- Being followed or threatened

Potential victim of domestic violence

- Victims of domestic violence can be at an increased risk of assault and harm

Young people

- Particularly children (those under the age of 18)

As a security operative, you need to carefully consider the implications for vulnerable children and young adults either using, passing or leaving venues or sites. You need to consider things like whether they require medical attention, whether they have friends or family nearby and whether they have all of their belongings with them. Think about whether they appear to be under the influence of drink or drugs, how old they are, who they are with, and whether it appears that they are being followed or harassed.

Other vulnerable people could also include those that:

- have a mental illness
- have learning disabilities
- have physical disabilities
- are elderly
- are acutely ill
- have invisible disabilities (physical, mental or neurological conditions that limit a person's movements, senses or activities and are invisible to the onlooker)

Indicators of child sexual exploitation

There are certain indicators that a child is being sexually exploited such as:

- children and young people in the company of older people or antisocial groups
- acting in an inappropriate and sexualised way
- being intoxicated
- arriving and departing a location with different adults
- getting into and out of several different cars

You must be vigilant at all times if you suspect a child is being sexually exploited, you must report it immediately and follow the organisation's policies and procedures.

Actions towards vulnerable people

In your professional judgement, if they appear to be vulnerable, you need to consider what help they might need. For example:

is there a relative or a friend close by to help them?

can you telephone anyone to come and help them?

can you call for a licensed taxi to take them home?

are there any local safe havens or other local initiatives such as those run by the St John Ambulance nearby?

can local street pastors or street marshals help them?

do you need to call the emergency services?

referral to other national or local initiatives (i.e. 'Ask Angela')

If in any doubt whatsoever, seek advice from a supervisor or call the police.

Learning outcome 2: Understand how to keep vulnerable people safe

Sexual predators

As a security operative, you need to be able to identify the behaviours that may be exhibited by sexual predators. It is important to remember that sexual predators don't look just one particular way but are all genders, shapes and sizes. Their behaviours could include:

- close monitoring of vulnerable people, e.g. someone looking lost or alone
- buying drinks for people who are already intoxicated or gifts for vulnerable people who may appear easy to groom
- suspicious behaviour around certain times and venues, e.g. loitering near a school at lunchtime or waiting for someone to pass by who looks vulnerable
- inappropriate use of technology, e.g. phones for upskirting (a photograph taken, usually without consent, underneath a woman's skirt or dress)

Indicators of abuse

There are several identifying indicators of abuse that security operatives can look out for, these can include:

- restricting freedom of individuals, e.g. the victim is not allowed to talk to anyone on their own
- unexplained bruising
- lack of confidence and insecurity – this may be someone you know that you have noticed has changed from a lively outgoing person to someone who is withdrawn
- change of personal circumstances, including cleanliness and general appearance

Allegations of sexual assault

Security operatives regularly wear uniforms. Some people find this reassuring and may choose to tell the operative about the abuse that they have been subjected to. This is called a disclosure.

Every organisation has a policy on what action to take if a member of staff or customer discloses information to you. You must follow the procedures when dealing with allegations of sexual assault. You must in the first instance:

- safeguard the victim by making sure they have a safe space to stay that is separate from the assailant
- inform your manager or your supervisor as soon as possible
- notify the police
- record and document all information at the first opportunity

Anti-social behaviour

As a security operative, you should always try to be positive and productive in your attitude when dealing with members of the public that are demonstrating anti-social behaviour.

You should:

- follow your organisation's policies and procedures
- speak to the person
- explain the situation and the risks of the anti-social behaviour
- explain the consequences if the anti-social behaviour continues
- remain calm
- ensure that your colleagues know about the situation and that you have back-up if needed
- remain vigilant
- conduct high-profile patrols
- promote early intervention
- use positive, non-aggressive communication
- promptly report incidents
- accurately record incidents
- liaise with police and other appropriate agencies



Learning outcome 3: Understand terror threats and the role of the security operative in the event of a threat

Terrorism

Terrorism is the use of violence, threats and intimidation especially in the pursuit of political aims. It is used to create a climate of fear within a population, with the intent of bringing about a particular change.

Some terrorist groups work on an international basis, whereas others fight for domestic issues. Certain terrorists target just one particular organisation or company for a specific reason, while others may be more indiscriminate in their targeting.

Public, commercial and retail premises, as well as places of entertainment, could become targets of either a bomb threat or an actual terrorist attack. As a security operative, you will need to be aware of:

- what is currently happening around the world and in your particular area
- any recent terrorist attacks or threats
- the location of your own site in relation to other possible targets nearby
- whether the site itself is famous or important in its own right
- whether the site is significant to any terrorist groups or causes
- the vulnerability of the site to attack
- the current level of threat nationally



Counterterrorism measures will help to reduce the chances of a site becoming a target. Managers and security operatives can significantly reduce the threat by:

- being vigilant at all times
- maintaining good housekeeping
- properly using physical security measures
- making regular, obvious patrols of the site
- implementing strict access control procedures
- using effective search procedures
- visibly using CCTV systems
- reporting suspicions to supervisors or managers immediately

Non-urgent information about terrorism should be passed to the **Anti-Terrorism Hotline** on:



0800 789321 or 101

This line is covered at all times by specialist counterterrorism police officers. Terrorism can also be reported online at: www.gov.uk/report-terrorism

Urgent information should be passed on using the 999 system.

All reporting methods are equally valid as they will always be redirected to the right place.

Know what information emergency response require and have an awareness of emergency response times.

THREAT LEVELS

Threat levels are designed to give a broad indication of the likelihood of a terrorist attack.

CRITICAL

means an attack is highly likely in the near future

SEVERE

means an attack is highly likely

SUBSTANTIAL

means an attack is likely

MODERATE

means an attack is possible, but not likely

LOW

means an attack is highly unlikely

Threat levels themselves do not require specific responses, however it is important that you, as a security operative, are aware of the different response levels and what moving from one level to another means for the location you are working in and the plan that is in place.

www.mi5.gov.uk/threat-levels

Learning outcome 3: Understand terror threats and the role of the security operative in the event of a threat

In the rare event of a terrorist attack, security operatives should encourage members of the public to:

RUN

to a place of safety

HIDE

if you cannot run, hide

TELL

call 999 (response times may vary according to locations)

See, Check and Notify (SCaN) is a current awareness strategy that aims to help businesses and organisations maximise safety and security using their existing resources.

ACT Awareness e-learning has been developed to support the United Kingdom's Strategy for Countering Terrorism. This e-learning provides nationally recognised corporate CT guidance to help people better understand and mitigate against current terrorist methodology. This course is free to access via the following link: <https://ct.highfieldelearning.com/>

Common terror attack methods

Once terrorists have identified a target, the potential attack will be moved into the planning phase, this phase involves the gathering of information to identify vulnerabilities and levels of security, which will inform the preferred method of attack. If required, a period of training and rehearsal will precede the actual attack. The most current terrorist attack methodologies have included:

- marauding terror attack (MTA) including firearms, knives, blunt objects, etc.
- explosive devices, including improvised explosive device (IED), person-borne improvised explosive device (PBIED), vehicle-borne improvised explosive device (VBIED)
- vehicle as a weapon (VAAW), also known as vehicle ramming
- hazardous substances including chemical, biological and radiological (CBR)
- cyberattacks

Actions to take

The role that security operatives are expected to play during a terror attack will be outlined in the policies and procedures for the venue/site.

There could be occasions when a terrorist attack occurs without warning. In the unlikely event of this happening, you should encourage members of the public to keep safe by following the 'Run', 'Hide', 'Tell' principles.

- Consider your route, act quickly and quietly, insist others come with you but don't let their indecision slow you down. Once you've identified a safe route: **RUN**. Consider your route as you leave, will it place you in the line of fire, is it safer to wait for the attacker to move away before you continue?

- If you can't move to safety, **HIDE**. When finding a hiding place, consider your exits and escape routes, avoid dead ends and bottle necks. Try to find places with reinforced walls, try to lock yourself in a room and move away from the door, be as quiet as possible, switch your mobile phone to silent and switch off vibrate. Don't shout for help or do anything that will give away your hiding place. The best hiding place with protection from gunfire will have a substantial physical barrier between you and the attacker.
- If you're able to evacuate, get as far away from the danger area as possible, try to stop others from entering but only if this won't put you in danger. Call the police, dial 999 and **TELL** them clearly the location of you and the attackers, descriptions of the attackers: their clothing and weapons, information about casualties and building access. Include anything else you think is important.

Security operatives may need to evacuate or invacuate the venue/site. Being aware of the organisation's procedures for both will help you to determine the course of action you need to take.

- **Invacuation/lockdown** – staff members and members of the public are moved to the most sheltered area of the venue/site away from windows and other exposed areas. All external doors and windows are locked.
- **Evacuation** – the orderly removal of staff members and members of the public to a safe place away from the immediate vicinity of the building. Evacuation will normally happen in situations such as a fire.

As a security operative, you need to remember that an early assessment of the situation is vital. If a terrorist attack begins outside, a quick lockdown procedure could protect everybody inside the site/venue, however, if the lockdown procedure is slow, incomplete or causes a state of confusion, the threat could move into the site/venue, putting the people inside at great risk.

Learning outcome 3: Understand terror threats and the role of the security operative in the event of a threat

Invacuation and evacuation both have their pros and cons including:

	Pros	Cons
Invacuation	Locks staff and members of the public away from the perpetrator, providing a physical barrier.	Potential lack of exits limits the ability to run should the perpetrator gain access or the attack zone spreads.
Evacuation	Allows staff and members of the public to get as far away as possible from the scene of the incident.	Some evacuation routes may put staff and members of the public at risk of being in the line of fire, or the perpetrator may attempt to pursue along the evacuation route.

As a security operative, you must have knowledge of the location you are working in, and make dynamic decisions based on available information to keep yourself and the public safe.

Public sector counterterrorism experts:
National Protective Security Authority (NPSA)

<https://www.npsa.gov.uk/>

National Counter Terrorism Security Office (NaCTSO)

www.gov.uk/government/organisations/national-counter-terrorism-security-office

Suspicious packages

As a security operative, you need to be aware of suspicious packages and the procedures to follow should one be identified. You need to know what looks out of place at the venue you are working at. Using the H.O.T protocol will help you to determine if the items are suspicious or not.



HIDDEN - has someone deliberately tried to conceal it from view?



OBVIOUSLY SUSPICIOUS - does its appearance seem odd or out of the ordinary? Maybe it's even showing wires, batteries, or liquids?



TYPICAL - is it typical for the location? For example, a large rucksack would be expected at an outdoor festival, but would be out of place at an indoor concert venue.

If you come across a suspicious package, you will need to double check your concerns by asking people/customers or other members of staff in the area if they know who it belongs to. If you're still not happy then there are simple immediate actions that you must follow.

- First, don't touch the item. If you've gone through the H.O.T protocol and think it's suspicious, any contact with the item could be very dangerous.
- Take charge, be polite but firm, and start to move people and yourself to a safe distance away from the item, even for a small package, like a briefcase, you need to clear 100m around the object, starting from the centre and moving out. Large items or small vehicles need a clear area of around 200m and large vehicles 400m or the length of a football pitch.
- Try to keep yourself and other people out of line of sight of the item, it's a broad rule but, generally, if you can't see the item, then you're better protected from it should it prove to be dangerous. Also, think about what you can hide behind, pick something substantial, and keep away from glass, such as windows and skylights.
- Communicate - who do you need to tell about the current situation? Include the police within those that need to be informed, however, some explosives can be triggered by the signal from a phone or radio. So, don't use mobile phones or walkie-talkies within 15m of the item (that's about the length of a bus).

It is vital to identify what the threat level is and where it is before any **invacuation** or **evacuation** decisions are made.

Learning outcome 3: Understand terror threats and the role of the security operative in the event of a threat

- If you have to leave to get help, first, cordon off the area to make sure people don't get too close to the item. You'll need to do this anyway to control access to the area. Members of the public should not be able to approach the item until it is deemed safe.
- Finally, try and keep eyewitnesses on hand, if the item was reported to you by a customer/visitor or a staff member ask them to stay close so they can tell the police what they saw.

The 4 steps to remember are:

- confirm if the package is suspicious
- clear the area as best you can
- communicate to your team and the police
- control others getting into that area

Suspicious activity

Suspicious activity is any observed behaviour that could indicate terrorism or terrorism related crime. As a security operative you will need to be familiar with the different methods of observing suspicious activity.

Hostile reconnaissance is the term used to describe how terrorists gain information on potential targets. They will often visit potential targets a number of times prior to an attack to try to find out as much as they can about the location itself, and to discover the best time and method of attack. You need to be vigilant at all times when working as a security operative, as you must try to recognise suspicious behaviour that may indicate a terrorist interest in your site.

You should use your customer service skills to disrupt potential hostile reconnaissance, having a professional, visible presence is a tool that all security operatives can use to deter hostile reconnaissance.

Suspicious behaviour may include:

- a particular interest in the outside of the site
- an interest in the CCTV systems and other security measures that are in place
- parked vehicles with people inside
- empty parked vehicles left unattended for long periods
- making unusual requests for information
- individuals avoiding security staff
- taking pictures of the site (overtly/covertly)
- making notes or drawing diagrams of the site
- taking an interest in the timings of activities
- false alarm activations (testing response times)
- damage to perimeter security
- breaching restricted areas
- attempts to disguise identity/ inappropriately dressed for the season/ location
- trespassing or loitering with no good reason
- tampering with utilities
- individuals carrying out activities inconsistent with the nature of the building or area
- asking unusual or very specific questions about the site or security arrangements
- nervousness
- reluctance to be noticed or seen
- multiple sightings of the same suspicious person, vehicle or activity
- use of forged/altered or stolen identity documents/carrying large amounts of cash

Learning outcome 3: Understand terror threats and the role of the security operative in the event of a threat

There are actions that can be taken to deter or disrupt hostile reconnaissance, including:

- ensuring a visible presence of vigilant security staff
- regular patrols by security operatives
- maintaining organised search procedures
- ensuring emergency exits are secured when not in use to prevent unauthorised entry

Responding to suspicious behaviour

Don't be afraid of taking action, have the confidence to ACT. Your actions could help avert an attack and save lives. If you see suspicious behaviour in work, then ACT immediately - report it to your line manager, supervisor or the venue manager and the police.

- If you feel it is a life-threatening emergency, you can report it by calling 999 and providing the operator with the following information:
 - your place of work and the specific building
 - location of the suspicious package inside the building
 - whether all customers and employees have been evacuated from the building
- You can also contact the confidential anti-terrorist hotline on:



0800 789321

- Or use ACT (Action Counters Terrorism) online reporting:
<https://act.campaign.gov.uk/>
- If you feel it is a non-emergency, then dial 101

See it. Say it. Sorted.

The British Transport Police's nationwide campaign, designed to encourage train passengers and people visiting train stations to report any unusual items or activity. Passengers and visitors can report any issues by texting **61016** or by calling **0800 405040**.



Appendix 1

Definitions - Working within the private security industry

Private Security Industry

**Access and egress control:**

a method or system of restricting access to and exit from a particular property or site by unauthorised people or vehicles.

ACS:

the SIA's approved contractor scheme.

Arrest:

the taking or restraint of a person from his liberty in order that he shall be forthcoming to answer an alleged crime or offence.

Assignment instructions (A.I.s):

documents that are used to describe what the client requires of the security company. Primarily used for security sites and retail sites. Assignment instructions are not commonly used in licenced premises.

Authorised persons:

agencies that are allowed to enter a site to carry out their duties.

CCTV:

A basic closed-circuit television (CCTV) system is a fixed communication link between a camera and a monitor.

Civil laws:

rules that help govern our daily lives.

Communication:

the imparting or exchange of information, ideas or feelings between human beings by speech, body language, gestures, behaviour, writing or other means.

Confidential information:

information that must be kept securely so that unauthorised people do not have access to it.

Criminal laws:

prevent people from committing more serious offences, usually against people or property, and punish people when those laws are breached.

Customer care:

how we deliver our services and how we provide security to our customers on a day-to-day basis.

Direct discrimination:

when someone is treated less favourably than another person because of a protected characteristic they have or are thought to have, or because they associate with someone who has a protected characteristic.

Emergency:

any unplanned incident that is so serious that it must be dealt with immediately.

Evidence:

information that may be presented to a court to decide on the probability of some point in question and particularly as to how it may determine a person's guilt or innocence.

False alarm:

a false report of an emergency, causing unnecessary panic and/or bringing resources (such as the security/emergency services) to a place where they are not needed.

Hazard:

something with the potential to cause harm.

Hostile reconnaissance:

how terrorists gain information on potential targets.

HSE:

the Health and Safety Executive.

Indirect discrimination:

when a policy or practice which applies to everyone particularly disadvantages people who share a protected characteristic.

Invacuation:

the controlled process of moving people to somewhere safe inside a building when there is danger outside or in another part of the building.

Lawful occupier:

someone who owns, occupies or has control over the property.

Appendix 1

Definitions - Working within the private security industry

Manned security:

where one or more security operatives work on a site providing both a deterrent against crime and an immediate response to incidents as they occur.

Marauding terrorist attack:

Fast-moving, violent incidents where assailants move through a location aiming to find, kill or injure as many people as possible. Attacks can be carried out using a variety of weapons, including firearms, knives and blunt objects.

PACE:

Police and Criminal Evidence Act 1984.

PPE:

personal protective equipment.

Physical security:

physical deterrents such as locks, alarms, barriers, grilles to help reduce crime.

Prejudice:

a hostile attitude towards someone who belongs to a certain group, simply because they belong to that group and are therefore assumed to have all of the characteristics ascribed to that group.

RIDDOR:

Reporting of Injuries, Diseases and Dangerous Occurrences Regulations.

Risk:

the likelihood of harm occurring.

Risk assessment:

the identification of hazards, the calculation of risk and the reduction of that risk, either completely or to an acceptable level.

Sec.3 Criminal Law Act:

using such force as is reasonable in the circumstances in the prevention of crime, or in effecting (or assisting in) the lawful arrest of offenders, suspected offenders or persons unlawfully at large.

Security:

a state or feeling of being safe and secure.

Security operative:

the general term used throughout this book to describe any person providing any kind of manned security to a client or premises.

Self-defence:

if any person has an honestly held belief that he or another is in imminent danger, then he may use such force as is reasonable and necessary to avert that danger.

Sexual predators:

persons who commit sexual crimes, very often targeting vulnerable children and young adults.

SIA:

the Security Industry Authority.

Stereotyping:

lumping certain groups of people together, assuming that they are all the same simply because they belong to that group.

Systems:

electronic and other technical systems to monitor premises for crime and other dangers, such as intruder alarms, fire detection systems and closed-circuit television (CCTV) systems.

Terrorism:

the use of violence, threats and intimidation in the pursuit of political aims.

Trespass:

committed by a person who is improperly on someone else's property without consent.

VAAW:

vehicle as a weapon.

Vulnerable person:

anyone who may be at risk from harm.

Workplace violence:

any incident in which a person is abused, threatened or assaulted in circumstances relating to their work.

Private Security Industry



Notes

Notes

Notes

The Principles of Working as a Security Officer in the Private Security Industry (Refresher)

Highfield Icon, First Point,
Balby Carr Bank, Doncaster,
South Yorkshire, DN4 5JQ, UK

© 2024 Highfield Products Limited

Follow Highfield on:



01302 363277 www.highfieldqualifications.com info@highfield.co.uk

Find out about our
upcoming webinars!

