Chapter 1: The main characteristics and purposes of the private security industry

The SIA has 3 main aims:

1. The compulsory licensing of individuals undertaking designated activities within the private security industry
2. To recognise quality service by managing the voluntary Approved Contractor Scheme (ACS)
3. Introduction of business licensing for all regulated security companies

The key purposes of the private security industry

Security is a state or feeling of being safe and secure. The UK's private security industry provides manned and technical protection in an effort to prevent and detect crimes and other unauthorised activities and raise standards within the industry.

As well as protecting premises, people and their property, security operatives also help to prevent and detect crime, prevent or reduce loss, waste and damage, as well as monitoring and responding to safety risks.

Security can be provided to clients in 3 main ways:

- **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
- **physical security** – physical deterrents such as locks, alarms, barriers and grilles to help reduce crime
- **systems** – electronic and other technical systems used to monitor premises for crime and other dangers, such as intruder alarms, fire detection systems and closed-circuit television (CCTV) systems

A 'security operative' is the general term used throughout this book to describe any person paid or used to provide any kind of manned security to a client or premises. This term includes door supervisors, uniformed security officers (including key holders), store detectives, CCTV operators, cash and valuables in transit operatives and close protection operatives.

The professionalism within the private security industry, alongside the licencing regime of the security industry authority, are both aimed at raising standards within the sector.

The aims and functions of the Security Industry Authority (SIA)

The organisation responsible for regulating the private security industry is the Security Industry Authority (SIA). The SIA is a non-departmental public body reporting to the Home Secretary, under the terms of the Private Security Industry Act 2001. Its mission is to protect the public by regulating the industry effectively through individual and company licensing, to remove and reduce criminality, to raise standards, to recognise quality of service and to monitor the industry generally.

The SIA's main functions are to:

- protect the public and regulate the security industry through licensing
- raise standards (through the Approved Contractor Scheme)
- introduce business licensing for all regulated security businesses
- monitor the activities and effectiveness of those working in the industry
- set and approve standards of conduct, training and supervision within the industry
- keep under review the private security industry and the operation of the legislative framework
- increase customer confidence

Chapter 1: The main characteristics and purposes of the private security industry

Licensable roles under the Private Security Act

Door supervisors – those who carry out security duties in or at licensed premises (for example pubs and nightclubs), preventing crime and disorder and keeping staff and customers safe.

Security officers (guarding) – those who guard premises against unauthorised access or occupation, outbreaks of disorder, theft or damage. They may also guard one or more individuals against assault or injuries that occur as the result of the unlawful conduct of others. This protection is given by providing a physical presence or by carrying out a form of patrol or surveillance to deter crime.

Security officers (key holding) – key holding is where a security officer keeps custody of, or controls access to, any key or similar device for operating (whether mechanically, electronically or otherwise) any lock.

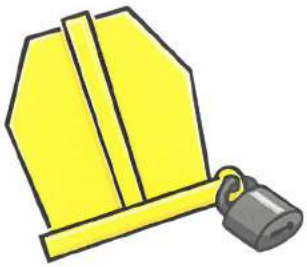
Cash and valuables in transit operatives – those who guard property against destruction or theft while using secure transportation of the property in specially manufactured vehicles.

CCTV operators – those who carry out guarding activities using closed circuit television equipment to either monitor the activities of members of the public in a public or private place or to identify a particular person. This includes the use of CCTV to record images to be viewed on non-CCTV equipment.

Close protection operatives – those who guard one or more individuals against assaults or injuries that might be suffered as a consequence of the unlawful conduct of others.

NI

Vehicle immobilisers are only licensed by the SIA in Northern Ireland. These are security operatives who either remove or relocate vehicles, restrict the movement of vehicles using a device or release vehicles after demanding or collecting a charge.



Other as yet non-regulated sectors of the private security industry include private investigation, event security, electronic security and fire systems.

Chapter 1: The main characteristics and purposes of the private security industry

Furthermore, security operatives must always conduct themselves in strict accordance with the SIA's **standards of Behaviour** for their particular role within the industry, as well as their own organisation's values and standards. For further information about the SIA, please visit: **www.sia.homeoffice.gov.uk**

Individual licensing

SIA licensing currently covers door supervision, security guarding, key holding, CCTV operations, cash and valuables in transit operations and close protection. Licensing ensures that security operatives are 'fit and proper' persons who are properly trained and qualified to do their jobs. The SIA also sets and approves standards of conduct, training and supervision within the industry.

Anyone wishing to work as a security operative must have an SIA licence before they start work. To work without a licence is a criminal offence, carrying fines of up to £5,000 or up to a 6-month prison sentence.

It is also a criminal offence for an employer to use an unlicensed security operative. To get a licence, you need to apply to the SIA itself. Your identity will be verified, you will be required to undergo the specified training, your criminal record will be checked and you will be required to pay a licence fee. Your licence will last for 3 years, after which time you will need to renew it.

Approved Contractor Scheme

The SIA's Approved Contractor Scheme (ACS) introduced a set of operational and performance standards for private security companies.

Companies that can prove that they can meet these standards can be awarded Approved Contractor status, which provides their customers and clients with independent proof of the company's commitment to quality.

Standards of behaviour

It is very important that all security operatives conduct themselves professionally at all times. Clients and members of the public expect security staff to act in a certain way.

But what qualities should security operatives possess?

Security operatives should be:

- professional
- polite
- sensitive
- honest
- reliable
- responsible
- courteous
- fair
- dedicated
- alert
- observant
- helpful
- approachable
- smart in appearance
- tactful
- self-disciplined
- cooperative
- patient
- loyal
- positive
- good communicators
- effective problem solvers
- team players
- handle sensitive situations

Above all security operatives should have integrity and be prepared to take responsibility for their actions.

Chapter 1: The main characteristics and purposes of the private security industry

Community safety initiatives

Working with the various private and community crime reduction initiatives in the area can go a long way towards helping security operatives keep their premises and clients safe.

This is done by helping to reduce the opportunities for crimes to take place. For example, local authorities now use Safer Community Partnerships to help reduce crime and the fear of crime in their areas. They work together with the police, the other emergency services and other relevant public and private organisations to try to reduce crime, public disorder, reoffending, anti-social behaviour, substance misuse and vandalism.

Working with national and local crime reduction initiatives like these can help security operatives to raise levels of security for themselves, the public and for their own clients and customers, as well as helping to reduce crime, disorder and anti-social behaviour in the area generally. Sharing information with these other initiatives and groups can also help to improve a security operative's knowledge of what is happening in the area in which they are working.

Crime reduction initiatives try to do this by:

- improving the physical security of vulnerable areas
- improving the environment itself
- removing the means and opportunities to commit crime
- using extra lighting to improve visibility in an area
- using warning signs
- controlling access to certain areas at specific times
- using CCTV
- using radio communications between various organisations and companies
- making use of local and national Pubwatch and Shopwatch initiatives
- using the yellow and red warning cards in conjunction with the local Pubwatch policy

How assignment instructions support the security operative role

The documents used to describe what the client requires of the security company are known as assignment instructions (A.I.s). They are primarily used for security sites and retail but are not commonly used in licenced premises.

Assignment instructions will state when certain duties, such as a patrol, must be carried out.

They also state the emergency procedures, emergency contact numbers and the numbers of other key individuals that you may need to contact, e.g. maintenance contractors.

Assignment instructions are confidential and should never be discussed with individuals outside of the security team and your management.

Chapter 1: The main characteristics and purposes of the private security industry

Benefits of using CCTV

CCTV has become one of the most essential pieces of technology used to monitor sites/ premises.

Ideally, CCTV cameras should be monitored at all times while the business is functioning. The CCTV operator can then direct security operatives to points of high risk while monitoring their safety. This is a cost-effective method of deploying security resources while keeping staffing to a minimum level.

Many customers and staff find CCTV reassuring as the presence of CCTV is known to be a deterrent to some criminals. If used correctly, the footage can be used as evidence in court.

CCTV can also be used to assist in investigations, for example for accidents or thefts. This can prevent malicious claims against companies, for example if someone attempts to push a trolley up an unsuitable escalator despite having clearly seen the signage prohibiting this action. CCTV cannot, however, be used to spy on people.

All businesses must register their systems with the Information Commissioner's Office (ICO). The ICO regulate the use of CCTV systems and storage of all personal data via the Data Protection Act 2018.

At each entry point to the premises, there must be signage stating that CCTV is in operation, as well as stating the name and number of the responsible person. Only approved and trained persons can view live footage.

Storage of the footage must be secure and the images must only be retained for the time period stated on the approval. This is usually 28 days, but approved time periods may vary.

CCTV must not be used where people are likely to be in a state of undress, e.g. the toilet cubicle.

Limitations of using CCTV

The use of CCTV can frighten some people, as they may feel that their privacy is being violated. Some people will even avoid certain areas because they do not want their image to be captured.

The cost of CCTV equipment has decreased significantly over the last 10 years, however the initial outlay for good and sufficient equipment can still be cost prohibitive for some businesses.

Poorly positioned cameras are more likely to be damaged prior to the occurrence of an illegal act. A camera cannot prevent crime, and a damaged/vandalised camera cannot do anything.

The capability of the CCTV operator, and their familiarity with blind spots or poor lighting, is key when looking to gain footage that is acceptable for use in court and for maintaining the continuity of evidence.

Although a CCTV system needs a human being in order to be fully effective, sometimes that person may use the cameras for the unauthorised monitoring of friends or even just someone they like to look at. This is misuse of the equipment and is illegal in many cases.

1 What does the abbreviation SIA stand for?

2 Describe the THREE main aims of the SIA.

1

2

3

3 Identify FIVE standards of behaviour expected of a security operative.

1

2

3

4

5

Chapter 2: Awareness of the law in the private security industry

Civil and criminal law

The role of a security operative in the fight against crime is increasing. Because of this, and so that you can be effective in the workplace, it is important for you to gain a basic working knowledge of the law.

Laws are there to ensure that citizens abide by certain rules that are made to keep everyone safe. Laws tell us what people are and are not allowed to do and allow people to be punished if those laws are breached.

There are 2 main types of law in the UK, **civil law** and **criminal law**.

Criminal offences include:

- murder
- kidnap (abduction in Scots law)
- rape
- sexual assault
- assault
- drugs offences
- possession of weapons
- theft
- burglary (housebreaking in Scotland)
- fraud
- robbery
- criminal damage
- arson (wilful fire-raising in Scotland)
- firearms offences
- child abuse
- domestic abuse
- driving under the influence

Security operatives and other members of the public have powers of arrest for some of these offences as they are so serious.

The standard of proof in the criminal courts is 'beyond reasonable doubt'.

CIVIL LAW

Civil laws help govern our daily lives. They usually deal with disputes between people, companies or other organisations. They are there to right wrongs, and proceedings are usually started by the person or people who believe they have been wronged in some way.

They deal with things like money owed, family and matrimonial disputes, property disputes, breach of contract, employment law, personal injury cases, custody of children, adoption, libel and slander (known as defamation in Scotland). Cases are often remedied by way of compensation orders for loss or damage.

Civil cases are usually dealt with in the county courts, with more serious cases being heard in the High Court. In Scotland, civil cases are heard by the Sheriff Court with more serious cases being heard at the Court of Session. The standard of proof in the civil court is 'on the balance of probabilities'.

CRIMINAL LAW

Criminal laws, on the other hand, are there to prevent people from committing more serious offences, usually against people or property, and to punish people when those laws are breached.

Criminal laws come from either very old judicial decisions made in courts (common law) or can be found in Acts of Parliament (statute law).

Cases are normally brought by the state, often following an arrest, and prosecution is sought through the criminal courts. Guilty verdicts can result in fines, probation orders and terms of imprisonment.

Chapter 2: Awareness of the law in the private security industry

Trespassers

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

One of your duties as a security operative is to ensure that only suitable and authorised people are allowed into the premise. During the course of your duties, you may well have to ask people to leave the premises and as a last resort you may have to physically eject them if they refuse to leave when asked. This section explains the powers you have to deal with these types of situations.

Trespass is not normally a criminal offence. It is, however, an act of interference against the lawful occupier of any specific premises and can be actionable through the civil courts.

A 'lawful occupier' is someone who owns, occupies or has control over the property. In the case of private buildings like factories, shops, pubs or clubs, it means the owner, manager or person in charge of the property and includes any members of staff acting on their behalf, as well as any authorised customers or visitors. This would include security operatives, whose job it is to protect the premise.

Security operatives may ask people to leave a premise if they:

- have no right or reason to be there
- break criminal laws
- break licensing laws
- breach specific premise rules or conditions
- start to display unacceptable behaviour

When asking a member of the public to leave the premises, you should first ask them to leave and explain why, telling them why they are not allowed to be there, what law they have broken, what rule they have breached or how their behaviour has become unacceptable.

If they refuse to leave, you should repeat the request, informing them that if they refuse to leave they will either be physically removed or the police will be called.

If they still refuse to go, you should offer them one more chance to leave peacefully by saying something like, 'Is there anything else I can say to make you leave on your own?'. This gives them one more opportunity to change their mind and is also a good defensible statement that other people will hear that shows that you did everything possible to encourage the person to leave peaceably, before having to resort to the use of force to remove the person from the premises. If you are working with another security operative, it will also warn them that you are about to take action and will allow them to prepare themselves to assist with the ejection. If someone you have ejected from a site becomes violent or attempts to force their way back in, then you should call the police to assist.

It is also within the law that police officers can be called upon to assist with ejecting people who are refusing to leave, having been asked to by a lawful occupier, their employee or agent. They may use such force as may be required to effect their purpose.

If you need to eject someone from the premises you are protecting, then it should be reported to the person in charge of your duty immediately. To safeguard yourself against any subsequent malicious allegations, it should also be recorded as an incident.

It is obviously always better to try to use tact and persuasion to get an unwanted customer to leave the premises, only using force as a last resort. Even then, you must use no more force than is necessary to remove the person.

R.E.A.C.T.
explains the best way to remove a trespasser:

- **R** request them to leave
- **E** explain the reasons for the request
- **A** appeal for them to leave, explaining what will happen if they do not
- **C** confirm that they still refuse to leave peacefully
- **T** take action (eject)

As a last resort, you may have to physically eject the trespasser from the site. The law allows you to do this, provided that:

no more force is used than is necessary to remove the trespasser from the premises.

Chapter 2: Awareness of the law in the private security industry

SCO

The Trespass (Scotland) Act 1865 makes it an offence under Scots law to trespass. The legislation was amended under the Land Reform (Scotland) Act 2003 which established universal access rights to most (but not all) land. These reforms do not apply (hence why trespass remains an offence) to:
houses and gardens and non-residential buildings and associated land, land in which crops are growing, land next to a school and used by the school, sports or playing fields when these are in use and where the exercise rights would interfere with such use, land developed and in use for recreation and where the exercise of access rights would interfere with such use, golf courses (you can cross a golf course provided that you do not interfere with any games of golf), places like airfields, railways, telecommunication sites, military bases and installations, working quarries, construction sites and visitor attractions or other places that charge for entry are exempt and as such unauthorised access would be trespass.

SCO

Trespass in Licensed Premises in Scotland

Under Section 116 of the Licensing (Scotland) Act 2005 it is an offence for any person to refuse to leave licensed premises as follows:

- a person on any relevant premises who behaves in a disorderly manner, and refuses or fails to leave the premises on being asked to do so by a responsible person or a constable, commits an offence
- a person on any relevant premises who, after the end of any period of licensed hours, refuses or fails to leave the premises on being asked to do so by a responsible person or a constable commits an offence

Where a person refuses or fails to leave any relevant premises, then the door supervisor may remove the person from the premises and if necessary for that purpose, use reasonable force.

A constable must, if asked by an authorised person to assist in exercising a power conferred by subsection 3 (above) and
if the constable reasonably suspects the person to be removed of having refused or failed to leave as requested, provide the assistance asked for.

A person guilty of an offence under this section is liable on summary conviction to a fine not exceeding £1,000.

NI

In relation to trespass, the new criminal trespass law enacted under s128 of SOCPA, has made it illegal to trespass on certain designated military and nuclear sites in Northern Ireland. There is a common law offence of trespass against property and a criminal law offence of trespass/ harassment against the person, including assault.

Chapter 2: Awareness of the law in the private security industry

The Private Security Industry Act

The Private Security Industry Act 2001 was brought in specifically to regulate the UK's private security industry and to help raise the standards of the individuals and companies working within it. One of its main aims was to increase the public's confidence in the sector and to increase public safety.

The government formed a new corporate body called the Security Industry Authority (SIA) to do this.

The SIA now licenses security operatives, supervisors, managers, directors and company owners in the areas of door supervision, manned guarding, key holding, cash and valuables in transit, CCTV operations and close protection (and vehicle immobilisation in Northern Ireland).

This is to ensure that people employed within the industry are 'fit and proper' for their job roles.

The SIA also provides a public register of licensed individuals and maintains a list of its approved companies via the Approved Contractor Scheme (ACS).

The Private Security Industry Act also gives the SIA various powers of entry and inspection to ensure compliance, and lists specific offences and subsequent sentences for those caught breaching the act.

Equality and diversity in the workplace

As a security operative, in order to improve your image and level of professionalism, it is important that you are aware of and act correctly in relation to issues concerning diversity and equality. Security operatives provide a service and must provide the same quality of service to everyone. You must not **discriminate** against certain types of people when carrying out your duties. Discrimination is treating a person less favourably than another person.

Prejudice is having a hostile (or sometimes positive) 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.

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

Prejudices and stereotyping can be harmful when they are used to openly discriminate against people. As a security operative, you are reliant on the public for support and confidence, so it is important that your conduct is seen to be impartial and reasonable at all times.

Chapter 2: Awareness of the law in the private security industry

The Equality Act 2010
(Not applicable in Northern Ireland)

Previously, discrimination, equality and diversity were enforced by numerous separate pieces of legislation. Those laws were often confusing and some were outdated and ineffective.

The Equality Act received Royal Assent on 8 April 2010 and its core provisions came into force on 1 October 2010. The purpose of the Act is to provide a new legislative framework to protect the rights of individuals and to advance equality and opportunity for all. The new Act simplifies 9 pieces of legislation, bringing into existence a singular statute dealing with discrimination. Some of the old laws remain the same, while others have been changed or expanded. Some new elements have appeared for the first time.

The Equality Act prohibits discrimination on the grounds of:

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

These are known as the protected characteristics. It is illegal for employers, for example, to discriminate against any of these groups of people in the areas of recruitment, access to training, pay and benefits, promotion opportunities, terms and conditions, redundancy and dismissal.

Furthermore, employers now have to make reasonable adjustments to cater for the employment of disabled people.

Types of discrimination

Direct discrimination occurs 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.

Indirect discrimination occurs when a policy or practice that applies to everyone particularly disadvantages people who share a protected characteristic.

People's rights under this legislation can be enforced through the county courts, resulting in fines and/or compensation being awarded.

Discrimination can be hurtful, insulting and demeaning to the recipient, and is not acceptable from security professionals.

It is also made clear under the Human Rights Act that all people have the right to be free from discrimination.

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.

Chapter 2: Awareness of the law in the private security industry

The Data Protection Act 2018

The Data Protection Act 2018 enabled the General Data Protection Regulation (GDPR). The legislations cover any information related to a person or 'data subject' that can be used to directly or indirectly identify them. It can be anything from a name, a photo and an email address to bank details, social media posts, biometric data and medical information. It will also introduce 'digital rights' for individuals.

The GDPR manages how personal and sensitive information can be used, stored and passed on. These laws give you rights as an employee and also require you to treat individuals' information responsibly.

The regulation ensures that organisations maintain the protection of data. It makes sure that personal data held by organisations is kept confidential, processed lawfully, used only for the purpose it was intended, not kept longer than necessary and is accurate. The regulation gives individuals the right to see the data and information held about them. It also promotes greater accountability and governance by organisations, as evidenced by the 'accountability principle', which requires organisations to demonstrate that they comply with the data protection principles.

The data protection principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations. In short, Article 5 (1) of the regulation requires that personal data should be:

(a) Processed lawfully, fairly and in a transparent manner

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

(d) Accurate and, where necessary, kept up to date

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

(f) Processed in a manner that ensures appropriate security of the personal data

Data protection rules often apply to the use of written records and notebooks, as well as the use of body-worn cameras.

You can find more information about the General Data Protection Regulation 2018 here:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/?q=digital

Key tasks

1 Describe civil law and criminal law.

Civil law

Criminal law

2 Identify the key legislation relating to equality and diversity in the workplace.

3 Explain how the data protection regulation impacts your role as a security operative.

Chapter 3: Arrest procedures relevant to security operatives

Arrest and limitations of arrest

During the course of your duties as a security operative, you will occasionally come across evidence of, or be witness to, an offence for which a person will need to be detained pending the arrival of the police.

As a security operative, you have no special powers of arrest, only the same powers of arrest as any other member of the public when it comes to apprehending suspects for a variety of offences. This section will appraise you of those powers and procedures so that you will know what to do should the situations arise.

An arrest or apprehension can be defined as:

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

For any individual to deprive another of his liberty is one of the most serious responsibilities a person can accept, and for this reason, you must ensure that you act correctly when apprehending someone for an offence.

The various powers of arrest afforded to all members of the public, including security operatives, must be used with discretion and consideration. These powers should only be exercised when circumstances make it necessary, not just because they are available. They should always be applied correctly and responsibly and as a last resort.

The police have other powers of arrest, under warrant, for specific offenses. Security operatives do not require a warrant to carry out a lawful arrest under the following legislation.

The most common power of arrest that you will use as a security operative can be found within Section 24a of the Police and Criminal Evidence Act 1984 (as amended by the Serious Organised Crime and Police Act of 2005). This Act was brought in to address the difficulties of the numerous and varied powers of arrest from the past, and now provides a power of arrest for most criminal offences where such a power is necessary (Article 26 PACE (Northern Ireland).

The most useful piece of common law that you will use as a security operative, however, is the power of arrest for 'breach of the peace'.

Breach of the peace

A breach of the peace is a common law concept that has ancient roots.

In general terms it is considered to be:

'any disorder or disruption to the peace in public or in private that results in violence, threat of violence or provokes violence from another'.

The common law power of arrest for breach of the peace states that:

Any person (including a security operative) may arrest without warrant where:

(a) a breach of the peace is committed by the person arrested in the presence of the person making the arrest

(b) the person making the arrest reasonably believes that such a breach will be committed in the immediate future by the person whom he has arrested, although no breach had occurred at that stage

(c) a breach of the peace has been committed by the person arrested and the person making the arrest reasonably believes that a renewal of it is threatened

SCO

Breach of the peace in Scots law

Breach of the peace is a common law offence against society and is defined as 'conduct severe enough to cause alarm to ordinary people and threaten serious disturbance to the community'.

The words 'severe' and 'serious' above are an essential element of breach of the peace and therefore it is not considered a trivial crime.

Some breaches of the peace might be more 'minor', such as cursing or swearing in public, peering in a person's window or shop window and causing alarm to other people, or more serious incidents such as fighting in public or conducting oneself in a riotous or disorderly manner.

The common law crime of breach of the peace is that it can be committed by 1 or more people, so long as the conduct of the person or people is riotous or disorderly, while the conduct must be severe enough to cause alarm to ordinary people and threaten serious disturbance to the community ***(Common law)***.

This is a useful but **rarely used** power of arrest for a security operative, as it is not restricted with regards to where a breach of the peace may occur in order for the power to be used.

Under normal circumstances, if you witness a breach of the peace occurring on the premises, then you would remove guilty parties from the site or venue. The power of arrest would usually only be used if it was considered necessary to stop or prevent a breach of the peace from occurring on the premises, in which case the police should be called to help deal with the problem.

Anyone arrested for causing a breach of the peace would be handed over to the police in the normal way and if necessary, would be taken before a magistrate in court to be bound over to be of good behaviour.

SCO

Scotland: Arrest

A private citizen has some powers of arrest under common law as long as they are carried out with care. A wrongful arrest, even a citizen's arrest, can result in a claim for damages.

For a citizen's arrest under common law to be lawful, the crime witnessed must be serious and not merely a breach of the peace. The person carrying out the citizen's arrest must be certain that an offence has in fact been committed, through either witnessing it or being a victim of it.

Reasonable force can be used if the arrested person attempts to resist. The arrested person must be handed over to the police as soon as possible.

Arrestable offences are at common law and arrest is classified as 'citizen's arrest'. Serious offences include:

- culpable homicide
- rape
- serious assault
- indecent assault (sexual)
- robbery
- theft
- housebreaking
- opening lock-fast places
- fraud
- malicious mischief
- wilful fire-raising

Indictable offences

The majority of offences that you are likely to come across during the normal course of your duties as a security operative are those referred to as 'indictable offences' under statute law.

The limitations to powers of arrest

Under Section 24a of the Police and Criminal Evidence Act (PACE) 1984, (the Criminal Procedure (**Scotland**) Act 1995, S26a of the Police and Criminal Evidence (Northern Ireland) Order 1989 (SI 1989/1341), certain serious offences have been given a special condition within criminal law and are known as indictable offences. The majority of crimes that security operatives come across will fall within this category. Indictable offences are those that may be tried at a Crown Court.

The reasons to arrest a person would be to prevent the person from:

(a) Causing physical injury to themselves or any other person

(b) Suffering physical injury

(c) Causing loss of or damage to property

(d) Making off before a constable can assume responsibility for him

Offences under this section, for which all security operatives have the same powers of arrest as other members of the public, include:

- murder/homicide
- rape
- assault (ABH, GBH and GBH w/i)
- sexual assault
- firearms offences
- drugs offences
- possession of offensive weapons
- robbery
- theft
- burglary
- fraud
- criminal damage

Chapter 3: Arrest procedures relevant to security operatives

The term 'citizen's arrest' is often used to describe a power of arrest given to 'a person other than a constable', although the term has no real meaning in law. These are exactly the same powers used by store detectives in retail establishments when they arrest shoplifters for theft, and the same powers regularly used by police officers when they catch suspects committing other serious offences.

SCO

In Scots law, neither store detectives, nor security guards can arrest for suspicion. They must have actually witnessed the crime of theft by using the following acronym, SCONE.

SCONE relates to retail loss prevention and store security.

It is the list of things that must be seen before a stop can be done.

- **S** **Selection** – the detective must see the customer take the item from the display
- **C** **Concealment** – the detective must see the customer conceal the item
- **O** **Observation** – the detective must maintain constant observation from selection to non-payment and exit. There must be no gaps in observation
- **N** **Non-payment** – the customer passes the last point of sale without making an offer of payment
- **E** **Exit** – the customer must be off the premises to prove the intention to permanently deprive

As a security operative, before you decide to arrest another person, you must be satisfied that you have reasonable grounds to suspect that the person is committing, or has committed, an offence which is classed as indictable. It is not always necessary for the suspected person to have actually been seen committing the offence, providing that there are 'reasonable grounds' to suspect that they had. It is, however, necessary that an indictable offence is being, or has been committed.

The term 'reasonable grounds' has no legal definition but is generally accepted as being that which can be explained to, and evaluated by, an objective third person. Reasonable grounds cannot be equated to mere suspicion.

How to arrest

As previously explained, an arrest is the 'taking or restraining of a person from his liberty in order that he shall be forthcoming to answer an alleged crime or offence'. Security operatives should only arrest someone for the following reasons:

(a) To prevent an offence being committed

(b) To prevent the continuance of an offence

(c) To prevent the renewal of an offence

(d) To detain someone for an offence already committed

Once the decision has been made to arrest someone, the person must be told:

- who you are (if not obvious)

'I am a member of the security team here'

- that they are under arrest

'You are under arrest.....'

- what they are being arrested for

'.....for criminal damage'

- the grounds for the arrest

'I have just seen you breaking that window'

- that the police will be called

'We are calling the police and you must wait here until they arrive'

Chapter 3: Arrest procedures relevant to security operatives

Where possible, arrests should be made as quietly and as discreetly as possible, preventing the escalation of situations to a point where they are out of control. As a security operative, you should take care not to show an over-aggressive attitude when effecting an arrest, just a firmness of intent.

It is perfectly acceptable to arrest someone without laying hands on them if the situation allows, but in many circumstances where security operatives make an arrest, there is the obvious possibility of being assaulted by the suspect.

Anyone you arrest should be treated in a reasonable manner. If, during the subsequent police investigation, it transpires that the detained person is innocent of the offence for which you arrested them, they are far less likely to take civil court action out against you if they were treated reasonably during the initial arrest.

Following an arrest

Having arrested someone, you are then responsible for the suspect's welfare and safe custody until the arrival of the police.

You must not lose sight of the person or allow them to be alone for any reason. There could be an escape attempt, or the suspect, aggrieved at their detention and pending prosecution, could assault either yourself or any other person nearby. Be aware also for the suspect's attempts to discard evidence. It is also not unknown for suspects to injure themselves or attempt to commit suicide if left alone for any length of time.

On the arrival of the police, you will be required to tell the officer what you have seen and done with regards to the arrest and why you have made the arrest. This is also the time to hand the police details of any witnesses to the offence, as well as any CCTV or other evidence in relation to it, such as weapons, drugs or stolen property. Provided that the officers are satisfied that there are sufficient grounds to arrest the person themselves, they will then formally arrest the person and take them from you. At some stage, possibly at the end of your shift, you will be required to make a formal written statement relating to your evidence, but the police will help you with this. Whether or not a statement is required, the arrest needs to be properly reported internally at the earliest convenience.

If the person is subsequently charged with an offence, you may later be called to attend court to give evidence of what you saw and did.

Unlawful arrest

Various sections of the public, particularly store detectives, security officers and door supervisors, regularly use their powers of arrest in the course of crime prevention and detection. To date, there have been relatively few successful civil or criminal actions against them for unlawful arrest. Provided that discretion and common sense are used in deciding when to effect an arrest, and that when you are making the arrest you have reasonable grounds to suspect that the person is either committing or has committed an indictable offence, then you should not encounter too many problems.

Your safety

Never put yourself in any unnecessary danger while effecting an arrest. If you are in any doubt about your ability to make the arrest, or about your personal safety, then the police should be called to assist or to make the arrest themselves.

Chapter 3: Arrest procedures relevant to security operatives

The use of force

Occasionally, you will need to use force to carry out your duties as a security operative, and under certain circumstances you are legally empowered to do so. The law gives certain situations when members of the public are allowed to use force on others, and the authority for security operatives to use force when necessary can be found in the following parts of the law.

Common law - the rules of 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.'

SCO

In Scots law, if a person is attacked, or is in reasonable fear of attack, he's entitled deliberately to use such force as is needed to ward off that attack.'

Furthermore, a person about to be attacked does not have to wait for their assailant to strike the first blow. Circumstances may justify a pre-emptive strike. This essentially means that if, while carrying out your duties as a security operative, you feel that you or someone else is about to be hurt, then you are allowed to use force to protect yourself or that other person.

In a criminal case in 1988, it was said that common law has always recognised the right of a person to protect themselves from attack and to act in the defence of others, and if necessary, to inflict violence on another in so doing. Provided that no more force is used than is reasonable to repel the attack, such force is not unlawful and no crime is committed.

In another case in 1995, it was said that the necessity of using force was a question for the subjectivity of the defendant, whereas the degree of force was more objectively considered by the courts. This means that security operatives have to decide themselves if and when to use force, whereas ultimately a court may have to decide whether the amount of force used was reasonable or not.

The questions that are likely to be asked about any use of force are:

1. Was there a need to use the force?
2. Was the amount of force used reasonable or not?
3. What was the extent of the injuries compared to the amount of resistance given?
4. What was the size and build of the injured party compared to the security operative?
5. Were any weapons used or threatened by the other party?
6. At what stage did the security operative stop using the force?
7. Was the force applied in good faith or in a malicious way?

COMMON LAW - preventing a breach of peace and saving life

'Any person may use such force as is reasonable in the circumstances to prevent a breach of the peace or to save life'.

In another 1981 case, it was said that in relation to stopping a breach of the peace, every citizen in whose presence a breach of the peace is being, or reasonably appears to be about to be committed, has the right to take reasonable steps to make the person who is breaking or threatening to break the peace refrain from doing so. These steps may include the use of reasonable force. Once again, though, what force is reasonable will depend on the facts of the particular situation. Security operatives are also allowed to use force to save someone's life. If, for example, an assailant is running at another person with a knife, then you would be entitled to use force to stop the assailant from killing the other person.

Chapter 3: Arrest procedures relevant to security operatives

SEC.3 CRIMINAL LAW ACT, 1967

This act gives everyone, including security operatives, the authority to use:

'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.'

The 'prevention of crime' element applies to any crime where the preventative use of force is reasonably required. This would include protecting property from damage or theft and protecting people from physical injury. This piece of legislation again allows you to use force to stop a crime from being committed, such as breaking up a fight (assault) or stopping someone from smashing a window (criminal damage), and also allows you to use force if needed to arrest someone and to stop them from running away before the police arrive.

It is important to remember that the wording of this act refers to:

'such force as is reasonable in the circumstances',

and previous criminal cases have pointed out that where force is used in these situations, the amount of force used must be judged according to the particular circumstances. It is made very clear, however, that the excessive use of force is not allowed. If you consider that every time you use force against another person you may well have to justify your actions, then you should be able to act reasonably in any given situation. If, however, you are reckless as to how much force you use, or you deliberately use excessive force, then you will have to answer to the police and possibly even to a court.

Security operatives are also allowed under the rules of trespass to physically eject members of the public from a site or venue when all other methods of persuasion have failed. You can effect lawful arrests for a variety of offences and you are allowed to protect yourself if you are attacked. What the law does not allow is the excessive use of force or causing unnecessary or malicious injuries to any person.

Security operatives must always be able to justify their actions. If you remember this during every potential confrontation with a member of the public, then you should prove to be effective within the security function.

Key tasks

1 Explain what is meant by the term 'arrest'.

2 Provide SIX examples of offences for which a security operative can make an arrest.

1

2

3

4

5

6

3 Explain the procedures a security operative should follow after an arrest.

Chapter 4: The importance of safe working practices

Health and safety in the workplace

Every year, thousands of people in the UK are forced to take time off work due to health and safety-related issues. For some, this may only mean a few days off work, but for others it could mean long-term injuries or even death.

The vast majority of incidents can be avoided through better health and safety procedures. Health and safety procedures in our places of work need to be effective to keep staff, visitors and customers safe. Furthermore, there is specific legislation in place to ensure that proper health and safety procedures are enforced anywhere where people work or come to be served.

The Health and Safety at Work etc. Act 1974

(Health and Safety at Work (Northern Ireland) Order 1978) covers employers, employees, the self-employed, suppliers, people who control premises and visitors/customers who come onto the site. Those failing to comply with health and safety legislation face a range of penalties, and businesses can be closed for serious breaches.

Breaches of the legislation can be dealt with by either the Health and Safety Executive (HSE) or by the local environmental health practitioner (EHP) from the local authority. Breaches can result in:

- improvement notices
- prohibition notices
- criminal proceedings

Duty of care

Employers have a moral and legal duty of care to protect the health, safety and well-being of their employees and others, including customers and members of the public who might be affected by their business. Employers must do whatever is reasonably practicable to achieve this. Serious breaches of health and safety legislation can result in penalties of up to 2 years' imprisonment and/or unlimited fines.

Health and safety responsibilities

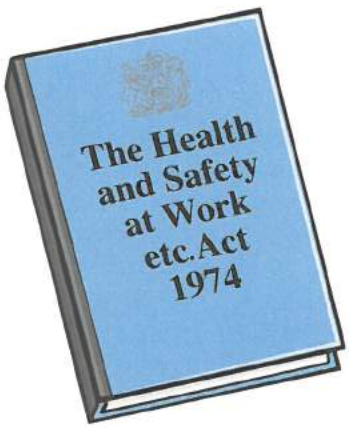
Employers must carry out a proper risk assessment of any possible risks to employees and other people visiting the site. Then they must do what they reasonably can to either remove or reduce those risks. They can do this by providing proper safety equipment, relevant warning signs, putting safe working practices in place, providing any relevant training or instruction and by supplying staff with any suitable personal protective clothing or equipment (PPE). They must provide safe access and egress as well as providing proper first-aid facilities, and ensuring that there are proper reporting procedures in place in case of incidents.

Depending on the size of the site and the number of people working there, they may have to also provide a written health and safety policy.

Employees and the self-employed

Employees and the self-employed working on the site, be they full-time or part-time, have a duty to take care of their own health and safety, and must make sure that they do not do anything that puts someone else's health and safety at risk.

Employees must follow the site's health and safety policy at all times if there is one in place, they should obey all safety instructions and should use safety and personal protective equipment properly. If serious incidents occur, they must follow the site's emergency procedures to help protect themselves, other staff and any visitors/customers. They must then follow the site's reporting procedures to inform the employer of any accidents and/or injuries.



Chapter 4: The importance of safe working practices

Workplace hazards and risks

Good health and safety practices in the workplace are all about reducing hazards and risks.

Definition

Hazard

Potential source of harm or adverse health effect on a person or persons.

Typical hazards in the workplace include:

- factors that cause slips, trips (e.g. unsuitable footwear), flooring, steps, uneven surfaces, spillages for example cleaning fluids and contamination, poor lighting

Risk

Likelihood that a person may be harmed or suffer adverse health effects if exposed to a hazard. Levels of risk may be, high, medium or low impact.

Typical risks in the workplace include:

- accidents due to poor lighting, uneven surfaces, steps etc.
- infection from body fluids
- dealing with aggressive or violent behaviour
- injuries from poor manual handling
- misuse/abuse of machinery
- sharp objects (needles/knives)
- diseases
- hazardous chemicals
- noise pollution
- moving vehicles
- obstructions
- fire/floods and other emergencies
- unsuitable footwear
- spillages, for example cleaning chemicals
- global or critical incidents

In relation to global (or critical) incidents such as pandemics, epidemics, acts of terrorism, etc. you must ensure that you follow all relevant health and safety policies and organisational procedures. In the case of a pandemic, you may find that you are required to work from home where possible, if this is not possible then you may be asked to wear additional PPE such as face masks when in the workplace. You can find further information on the .gov website and the World Health Organization website **https://www.who.int/** about current global incidents.

Minimising risks to personal safety and security

Once a hazard or risk has been identified, you need to follow the **hierarchy of control** to work out the best ways to deal with the potential problem. This is done by asking yourself:

- can the hazards be eliminated?
- can the hazard be substituted with a reduced risk?
- can the hazard be isolated or enclosed?
- would the introduction of a safe system of work reduce the risk? For example, new procedures and routines.
- would information, training or supervision reduce this risk?
- would PPE help?

Examples of personal protective equipment (PPE) for security operatives include:

- waterproof clothing
- high-visibility clothing
- headwear
- gloves (needle/slash resistant)
- rubber gloves and face shields (body fluids)
- stab-resistant vests
- ear defenders
- eye protection
- safety footwear
- face masks/coverings (infectious diseases)

There are 5 steps to carrying out a risk assessment

Step 1 Identify the hazards

Step 2 Identify who may be harmed and how

Step 3 Evaluate the risk and introduce further controls

Step 4 Record the findings and implement them

Step 5 Review and revise and update if necessary

Chapter 4: The importance of safe working practices

The 6 safe lifting techniques are:

1. Stop and think
2. Position the feet
3. Bend the knees
4. Get a firm grip, keep the back slightly flexed
5. Raise with the legs
6. Keep the load close to the body

Definition

Risk assessment

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

Equipment:

- metal detectors and/or mirrors for searching
- body-worn CCTV
- radios
- mobile phones
- personal alarms
- torches
- equipment as it applies to the incident e.g. to help control infections

Safe manual handling

Manual handling is the movement or support of any load by physical effort, including lifting, moving, carrying, pushing and pulling.

If you lift or move heavy objects without using the recognised procedures, you run the risk of sustaining the following injuries:

- fractures
- spinal disc injuries
- trapped nerves
- friction burns
- damage to muscles
- damaged ligaments and tendons
- abrasions and cuts
- hernias

It is important to follow safe routines and be systematic before attempting to lift a load, use

L I T E

to evaluate the risk.

L LOAD

Look at the load. If it is too heavy, can it be lightened or split?
If it is unstable, can handles be fitted or the load be reapportioned?

I INDIVIDUAL

Consider the capability of the person. Are they strong or fit enough? Are they adequately trained for the task?

T TASK

Evaluate the job to be done. Does the task involve stretching, twisting or bending? Can machinery be used or can team handling be used?

E ENVIRONMENT

Control the environment where the task takes place.
Is the floor slippery or uneven? Can the layout or floor condition be improved?

Lone working

Security operatives who work alone can be at particular risk in the workplace. They may feel isolated if they only have technological means with which to communicate with colleagues or call for assistance, technology can often fail to work in the manner intended.

Security officers could particularly be susceptible to:

- violence
- injury
- ill health
- lack of support/communication
- lack of welfare facilities for rest

Chapter 4: The importance of safe working practices

Safety signs and signals

Safety signs are used to communicate health and safety instructions. They must be kept clean, in good condition and must be displayed where they can be easily seen.

Security operatives must be aware of the colours and shapes of the 6 different types of signs.

PROHIBITION 1

Prohibition signs mean that you are prohibited from doing something.

MANDATORY 2

Mandatory signs mean that you must do something.

SAFE CONDITION 3

Safe condition signs indicate where to go to for safety.

WARNING 4

Warning signs indicate a specific danger.

FIRE SAFETY 5

Fire safety signs indicate firefighting equipment.

HAZARDOUS SUBSTANCE 6

Hazardous substances signs warn you about dangerous chemicals.

Reporting health and safety accidents and incidents

Following any accident or medical incident it is important to record all of the details relating to the situation. The information contained in the accident or incident book can help employers to identify accident trends, so they can then improve practices and procedures on the site to prevent further similar incidents.

These records may also be required for insurance and/or investigative purposes.

Reporting procedures

Accident and incident reports need to include at least the following information:

- day, date and time of incident
- location of incident
- how you were alerted to it
- what you saw
- what you were told
- what happened
- what action you took
- whether first aid was required
- whether the emergency services were called
- what the result was
- details of any injuries
- details of any witnesses
- any descriptions of property or people

These reports need to be made as soon as possible after the incident has finished, while the events are still fresh in your mind.

Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 2013

For serious accidents, incidents and near misses at work, **the employer** or the designated 'responsible person' is required by law to notify their local authority, the Health and Safety Executive (HSE) or the Incident Contact Centre. This can now be done online.

The first person on the scene assisting a casualty may not be directly responsible for completing the RIDDOR report, but they must ensure that their supervisor, manager or the health and safety officer within the company receives the correct information contained within the accident or incident report. Security operatives need to know the site's procedures for reporting medical incidents and must adhere to them.

NI

RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (Northern Ireland) 1997.

Chapter 4: The importance of safe working practices

Keeping personal information safe

The Data Protection Act/GDPR, covers any information related to a person or 'data subject' that can be used to directly or indirectly identify them. It can be anything from a name, a photo and an email address to bank details, social media posts, biometric data and medical information. It will also introduce 'digital rights' for individuals. As a security operative, it is vital that you keep all personal information safe. This can be done by:

- following all organisational procedures
- following assignment instructions
- maintaining confidentiality of information
- using social media in a responsible way; this includes having the highest levels of security settings on your accounts
- not wearing anything identifiable outside the workplace
- demonstrating personal vigilance, e.g. not completing surveys
- not discussing work issues outside the workplace
- not discussing work information with colleagues

1 Identify the responsibilities of employees and employers under the Health and Safety at Work Act.

Employees	Employers

2 Identify FOUR risks associated with lone working.

1

2

3

4

3 State the procedures that should be followed for recording and reporting accidents and health and safety incidents.

Accidents	Health and safety incidents

Chapter 5: Fire procedures in the workplace

Fire safety measures

As you saw in the health and safety section, both employers and all members of staff have a legal duty to do what they can to help keep everyone safe.

Fire safety on the premises or site is important for both staff and any visitors or customers. If a fire occurs in the workplace, it could result in the disruption of the normal business activities and can affect profitability. More importantly, staff and/or customers could be injured or even lose their lives.

Good fire safety is, therefore, everyone's responsibility. Basic fire prevention measures can go a long way towards helping to prevent the chances of a fire starting in the first place, for example:

- all non-essential electrical appliances should be switched off
- electrical points should not be overloaded
- all electrical equipment should be inspected regularly and maintained properly
- flammables must be stored safely
- ashtrays should be emptied regularly
- rubbish should be stored away from the building
- electric and gas fires must be kept well away from furniture

Under the **Regulatory Reform (Fire Safety) Order** of 2005, (Fire (Scotland) Act 2005) employers must nominate a competent person to carry out a full fire risk assessment for the site, which must be documented.

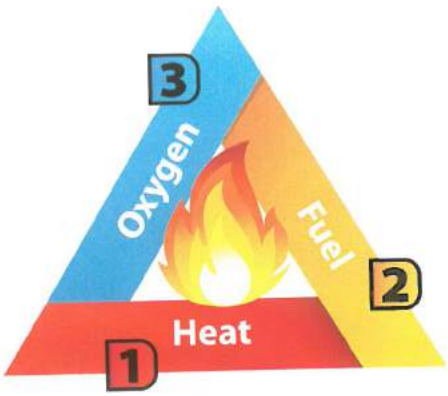
They must also provide their employees with any relevant information, instruction and training to ensure their safety while working on the site.

Employees such as security operatives must take responsibility for their own health and safety, and for that of others. They must be observant, vigilant and also cooperate with their employers in all matters relating to fire safety. This includes following any training and adhering to the fire plan.

Elements needed for a fire to exist

Fire needs 3 elements to start and survive. They are heat, fuel and oxygen. If any of these 3 elements are greatly reduced or removed, then the fire itself will be reduced or extinguished.

The fire triangle



This is known as the fire triangle. All 3 elements need to be present for a fire to start and continue. If any 1 or more of these elements are taken away, then the triangle is broken and the fire will die out.

Fire needs 3 elements:

1 **HEAT** - a minimum temperature is needed to start a fire, and for it to continue.

2 **FUEL** - fire needs something to burn, like solid fuel, oil or gas.

3 **OXYGEN** - fire needs oxygen to burn, as it supports the combustion process.

Classifications of fire

Fires are divided into types or classifications. Each class requires a different method of extinguishing and so it is important that we understand the differences.

	**CLASS A**	Ordinary combustibles, i.e. paper, wood, textiles, rubber, plastic, fabrics
	**CLASS B**	Flammable liquids, i.e. petrol, oil, paints and solvents
	**CLASS C**	Flammable gases, i.e. butane, propane
	**CLASS D**	Metal fires, i.e. magnesium, sodium
	**CLASS F**	Cooking oils and fats
		Fires involving electricity

Chapter 5: Fire procedures in the workplace

Information on fire extinguishers

*All extinguishers should be inspected annually by a competent person, e.g. an extinguisher engineer.

Actions on discovering a fire

It is important that all security operatives take the correct actions on discovering a fire. You will need to:

- follow the organisation's policies and procedures
- sound the alarm and inform emergency services
- follow the acronym of FIRE:
  - Find – you discover a fire
  - Inform – raise the fire alarm
  - Restrict – restrict access to the area of the fire
  - Evacuate – evacuate the building or extinguish (extinguish the fire if safe to do so).
- control panel: Important to ensure full understanding of the extent of the area of the incident, to pass on correct message to emergency services e.g. with regard to materials or chemicals stored in the affected area

Fire-fighting equipment

Fire extinguishers are generally used to fight small fires, to prevent them spreading and causing large-scale damage.

They have a limited capacity, but they can be easily carried to the fire and quickly put to work.

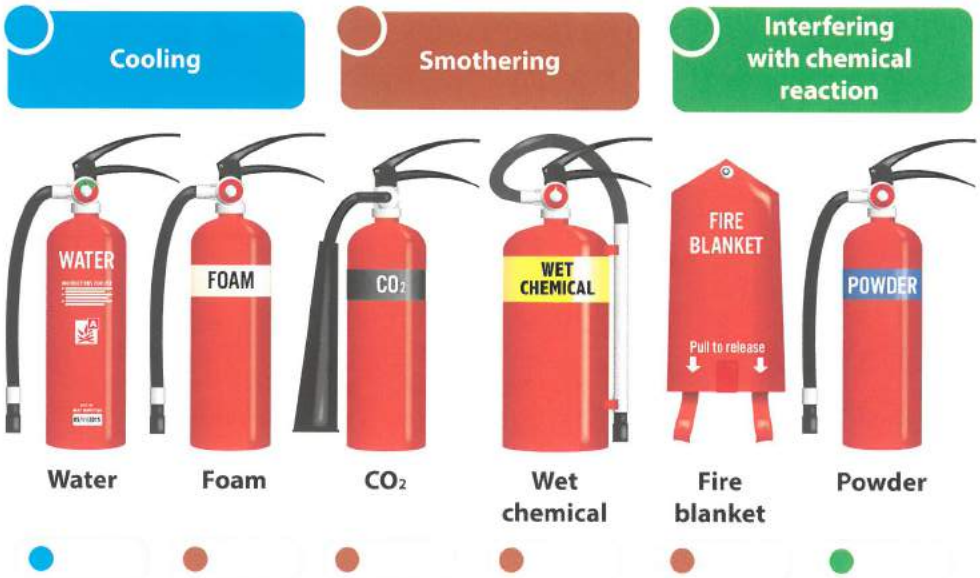
They are intended to be used by anyone who needs them, so it is important that all members of staff learn of their uses, locations and methods of operation.

Fire extinguishers should be sited in conspicuous locations on escape routes, such as next to exits and in corridors, and should be mounted on wall brackets.

Different types of extinguishers are designed to fight different classes of fire, so it can be useless or even dangerous to use the wrong type of extinguisher at the scene of a fire.

We need to understand, then, how the different types of extinguishers work and how they put out fires.

Fire extinguishers



Only attempt to fight a fire if:

- the alarm has been raised
- the emergency services have been contacted
- the fire is not spreading and has been confined
- you have a clear escape route not threatened by fire
- you have selected the correct extinguisher

Do not attempt to fight a fire if:

- it is bigger than a wastepaper bin (rule of thumb)
- you need more than 1 extinguisher
- the room is filling with smoke
- you do not have a clear escape route
- gas cylinders or chemicals are involved
- your efforts are not reducing the size of the fire
- you do not have the correct extinguisher

To operate an extinguisher:

- select the correct extinguisher
- check the contents gauge
- pull the pin to break the seal
- holding the extinguisher upright and squeeze the trigger
- test the range and content (away from the fire)
- extinguish the fire using the correct technique for that type of extinguisher and the nature of the fire

Chapter 5: Fire procedures in the workplace

Other firefighting equipment

Apart from fire extinguishers, there are several other types of equipment used to put fires out or to reduce their effects.

Fire blankets

Fire blankets can be used to extinguish fires by smothering them. They are often found in kitchens as they are very useful for extinguishing fat fires in pans.

Sprinklers

Some fire alarm systems are connected to sprinklers which spray water on to the fire from outlets in the ceiling, holding back the fire until the arrival of the fire brigade.

Hose reels

Hose reels are long lengths of rubber hose on large drums positioned strategically around the site. The hoses are permanently connected to the mains water supply and are started by opening a valve before use. They can be quite heavy to unreel when needed but are very effective when used as they provide a limitless supply of water.

Dry and wet risers

Some buildings, particularly multi-storey ones, have riser systems built in. These systems consist of long water pipes running along the outside of the building and across the ceilings on each floor, allowing water to be dispensed via sprinklers to each floor in the event of a fire.

Wet riser systems have water in the pipes all the time, whereas dry riser systems need to be activated manually to send the water into the pipes.

Flooding systems

Flooding systems are designed to be used in unoccupied rooms where there are high value contents or areas where a fire may cause major disruption to the activities of the organisation. Examples might be archives, electrical equipment or switchgear.

On detection of the fire, a fire extinguishing medium (most commonly CO_2) will be discharged into the room to replace the air and extinguish the fire by smothering.

Fire doors and fire exits

Internal fire doors are used to help prevent or reduce the spread of smoke and flames from one room to another. They should be closed at all times, unless they can be closed electronically if the fire alarm activates.

They should not be obstructed. Fire exits are vital as a means of escape in the event of a fire. They should be clearly marked, must be unlocked when anyone is in the building, and should not be obstructed on the inside or the outside.

Fire alarm control panels

These are the warning and controlling units within a fire alarm system. Once a possible fire emergency is detected within the building or somewhere on the site, usually as the result of a signal from a smoke or heat detector, the control panel alerts those monitoring it via various lights and audible alarms.

Chapter 5: Fire procedures in the workplace

Risk assessments will prescribe the site's own specific procedures for the action to be taken in the event of a fire.

Typical actions would include:

- raising the alarm - yelling fire to warn others
- operating the nearest manual call point (if fitted)

- calling the fire service (999)
- evacuating the area
- restricting access and isolating the fire
- reporting to the assembly point

- only attempting to fight fire if it is safe to do so and you have been trained

By understanding the layout of the control panel, security operatives can work out what type of an emergency it is, exactly where it is occurring and over what extent of an area.

A decision can then be made as to what appropriate action to take, be it to inform a supervisor and then search the area concerned, or to call the fire brigade immediately, and provide information about the incident itself and any secondary dangers there might be.

Some of the more sophisticated systems actually call the fire brigade, sound the fire alarm, unlock doors, cut off electricity and set off sprinkler systems automatically.

If you are required to monitor a fire alarm control system as part of your role as a security operative, then you need to properly understand how it works and what actions you personally need to take in an emergency.

Fire evacuation procedures

One of the most important roles for security operatives in the event of a fire will be ensuring that the site is evacuated quickly and safely.

Hopefully, both staff and visitors/customers will know to leave the building when they hear the fire alarm sounding. As a security operative, you must be available to encourage people to leave via the safest exit, and to assist anyone who does not seem to know what to do. Particular care needs to be taken to look after any vulnerable people like children, the elderly or those with physical or mental difficulties. It is also important to try to avoid causing unnecessary panic.

Security operatives need to take control of fire incidents in an assertive but calm manner. You need to show decisiveness, leadership and use clear, effective communication skills so that others understand how serious the situation is.

Security operatives also need to know where the fire assembly points are and what needs to be done once the building or site has been evacuated.

Evacuation procedures need to be practised.

Remember the 5 P's:

- P **PLANNING** and
- P **PREPARATION**
- P **PREVENTS**
- P **POOR**
- P **PERFORMANCE**

As a security operative, if you act promptly and correctly in times of emergency, you can help save time in the evacuation, keep yourself and others safe, assist the emergency services, prevent injuries and save lives.

Chapter 5: Fire procedures in the workplace

Fire wardens/marshals

Fire wardens (sometimes called fire marshals) are members of staff that are nominated to take responsibility for a particular area with regards to fire safety. The numbers of nominated wardens/marshals will vary depending on the size of the site and the numbers of people involved.

Under the Regulatory Reform (Fire Safety) Order of 2005, (Fire (Scotland) Act 2005) they are there to assist the designated person responsible for fire safety generally.

The actions to be taken by fire wardens/marshals in the event of a fire are detailed in the evacuation plan. Those duties will usually include:

- sounding the alarm/calling the fire service
- checking the allocated area to ensure that everybody has left
- taking control of the evacuation and ensuring that anybody with evacuation difficulties is aided
- proceeding to the assembly area and reporting to the fire officer in charge

Taking or assisting with the roll call.

The following list, although not exhaustive, details some of the specific roles usually given to fire wardens/marshals:

- assisting with fire risk assessments
- checking that all exit doors and escape routes are unlocked and unobstructed

- ensuring that all fire extinguishers are in the correct position with seals in place
- checking that all safety signs are clearly visible and in the correct place
- making sure that all alarm call points are unobstructed and working correctly
- checking that all fire doors are closed and functioning properly
- ensuring that corridors and walkways are kept clear
- ensuring that assembly points are clearly marked and easily accessible
- reporting any equipment faults

1 State the THREE elements needed for a fire to start and survive.

1

2

3

2 List FOUR tasks a fire warden/marshal may be required to carry out.

1

2

3

4

3 List FOUR classes of fire and their meaning.

1

2

3

4

Chapter 6: Emergencies and the importance of emergency procedures

Emergencies

An emergency is a situation that is unexpected and could threaten safety or cause serious disruption. An emergency requires immediate attention.

Emergencies can include incidents, occurrences and accidents, for example:

- **an incident/occurrence** could include a fight, power cut or drug overdose
- **an emergency** could include health emergencies such as epileptic seizure, anaphylactic shock, heart attack etc.
- **an accident** could include someone falling down steps or slipping on a wet floor

Responses and reactions to emergencies

You need to be aware that not all people react in the same way during emergency situations. Some may become hysterical and run away, others may just freeze on the spot, not knowing what to do. Both reactions could cause their own problems to the security team.

Fight or flight

It is important that you understand what happens to yourself and others when you are confronted by either conflict or by frightening or threatening situations. Only then can you plan what is the best way to react yourself and how to treat others when conflict arises.

If someone you are dealing with becomes angry and starts to threaten you, then you will automatically start to use the emotional side of your brain more than the rational side. It is the natural human response to a threat or potential threat to our well-being and safety.

If, as humans, we did not get frightened in such situations, our brains and bodies might not be prepared to be able to react quickly enough or in the proper way if we did actually need to protect ourselves.

When you become frightened, your body automatically enters what is called **fight or flight** mode.

This is because of the basic natural animal instinct that we all have, which helps us to survive potentially dangerous situations. When in fight or flight mode, various different things will automatically happen to your body to try to make you better prepared to deal with the threat, both physically and mentally.

Your body releases the hormone adrenaline into your system to increase your physical ability to fight or run away. This adrenaline rush increases your heart rate, pumping extra blood and oxygen to the muscles you need to use. Your eyes will widen to take in as much of the situation as possible, although sometimes you will centre your attention directly onto the threat itself, causing what is often called 'tunnel vision'.

Your sense of hearing will intensify, again to try to allow you to take in as much information about the threat as possible.

Once the situation ends, whether that is by you having halted or fought off the threat, or whether you have been able to get away from it, then your brain and body begins to calm down again, in an attempt to get back to normal. Your body will slowly return to its natural relaxed state, and as you calm down, your brain will return to thinking with the rational side again.

If your brain and body do not return to their natural conditions as they should, then you could go into a state known as shock. This usually only happens after a particularly threatening or frightening situation, however.

When dealing with an emergency situation, as a security operative you need to be aware of taking control in crowds or with large numbers of people present during an incident. This is to try to avoid people from being crushed or injured during an evacuation or invacuation.

Companies will often have an escalation procedure for incidents and emergencies. You must understand how a graduated response can be applied in each situation. You will be required to record your involvement and may be asked to review and evaluate the responses during the incident.

We can place incidents generally into three camps:

EMERGENCIES

URGENT

and

NON-URGENT

Emergencies are life-threatening incidents requiring immediate attention and probable deployment of emergency services.

FIGHT or FLIGHT

Fight or flight prepares our brains and bodies to:

stand and physically FIGHT fight off an attack

or to

run away from the situation FLIGHT to keep ourselves safe

Chapter 6: Emergencies and the importance of emergency procedures

Making emergency calls

If you need to call for the emergency services, call

999.

This will put you through to the emergency services operator. The operator will ask you for the following information:

- which service you require (police, fire, ambulance)
- the telephone number you are calling from (in case you are cut off or for a call back)
- your exact location (address and postcode)
- type of incident
- number of casualties
- extent of injuries
- any other dangers or hazards

You need to remain calm while making the call and you need to provide as much information about the incident as you can, so that the emergency service requested can provide the best response.

Types of emergencies within the workplace

Examples of emergencies that you may become involved with as a security operative include:

- power system or equipment failures
- floods
- actual or threatened serious injuries
- serious illnesses
- bomb threats
- fires
- terror threats

Actions to be taken in an emergency

All incidents need to be dealt with immediately, very often with the emergency services being called to attend. You will need to follow your company or site guidelines on how to deal with them.

Fires, floods, power cuts, gas leaks and chemical spillages are normally dealt with by activating the alarm and then evacuating the site. The emergency services should be called once the evacuation has been started.

In a situation where a gas leak is suspected, once the evacuation has been started you should try to ensure that no one smokes or switches on any lights or electrical equipment in the area, as even a small spark could cause an explosion.

Where possible, doors and windows should be opened to try to disperse the gas. If possible, the gas supply should be turned off at the mains.

Road traffic accidents are normally dealt with by the police. An ambulance may also be required if serious injuries are sustained.

Incidents of violence may be dealt with by removing the instigators from the site, by calling the police or by making arrests if serious injuries are sustained. First aid may also be required. Serious crimes that occur on the site will normally be dealt with by calling the police. Containing any suspects and crime scene preservation must also be considered. First-aid incidents, where staff or visitors/customers are injured or become ill, should be dealt with by a trained first-aider. In serious incidents, an ambulance should be called.

All bomb threats and suspect packages must be dealt with seriously, usually by raising the alarm, evacuating staff and visitors/customers via the quickest and safest exit and then by calling the police.

It is important that all security operatives know and follow correct procedures for any of these emergencies. You need to ensure your own safety as well as the safety of others in dangerous situations. You may need to call and assist any of the emergency services.

Most importantly, members of the public and other members of staff will look to you as a security operative for help during emergencies. You will need to take control of situations professionally and calmly and follow the correct procedures so that other people do what is safest and best for themselves until the situation is resolved.

Chapter 6: Emergencies and the importance of emergency procedures

Personal injury responses

First aid is defined as the initial or immediate assistance given to someone who has been injured or taken ill, before the arrival of an ambulance, a doctor or other qualified person.

Employers are required by law to provide adequate personnel, training, equipment and facilities to any staff or visitors/ customers should they be injured or taken ill on the site.

As a security operative, you must know your site's policy for providing first aid, what you are expected to do in a medical emergency and who the designated qualified first aiders are on the site. You may even be required to undergo first aid training yourself.

If you are trained to do so, you may be required to administer first aid in times of emergency. If you are first-aid trained, remember the following:

- ensure your own safety first
- assess the situation
- control the situation
- diagnose the injury/illness
- save life
- send for appropriate medical assistance
- keep people safe
- provide privacy

In a first-aid incident if you are not trained, you may need to:

- call the first-aider if you are not qualified (if you are, you may still need support)
- know when to call an ambulance; you or the first-aider may be able to deal with a minor injury, but it is very important that you know when to call an ambulance - always take guidance from a qualified first-aider
- ensure that onlookers are kept to a minimum but also monitor anyone who has remained for signs of shock
- provide as much of a physical block as you can, to protect the dignity of the casualty and prevent onlooking
- direct the ambulance to the casualty (if you are not the first-aider)

As mentioned previously, it is important to record all details relating to injuries sustained on the site, whether they are sustained through accidents or criminal actions.

The information contained in the accident book can often help employers to identify accident trends and improve the general health and safety of the site. These records may also be required for insurance and/or investigative purposes.

The main aims of first aid are to:

- preserve life
- prevent the condition from worsening
- promote recovery
- obtain qualified assistance

Chapter 6: Emergencies and the importance of emergency procedures

Evacuation and invacuation principles

When evacuating or invacuating a building, it is important that you are aware of the organisation's policies and procedures and specific requirements, these must always be followed to ensure customers and staff members are kept as safe as possible.

Evacuation – this is the controlled process of emptying an area or premises of people.

Evacuation can be to an adjoining area within a building or outside depending on the severity of the incident. Evacuation could be required in the event of a flood, fire or terror threat, for example.

There may be situations when invacuation needs to be completed.

Invacuation - this is the controlled process of getting people into safe premises due to an incident which could cause harm to people who are outside. For example, if a person with a firearm started to shoot people in the street, you would encourage everyone into the building and lock the doors for safety.

Different sites or venues may have different evacuation and invacuation procedures, as a security operative, you will need to make yourself aware of the policies for carrying out these procedures at each venue you work at.

Key task 6

1 What are the FOUR aims of first aid?

1

2

3

4

2 Identify FOUR types of emergency that could happen in the workplace.

1

2

3

4

3 Explain the principles of evacuation and invacuation.

Evacuation

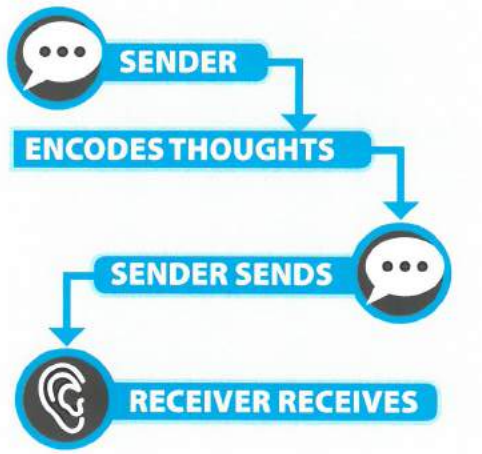
Invacuation

Chapter 7: How to communicate effectively as a security operative

The basic elements of communication

During the course of your duties as a security operative, you will regularly come into contact with members of the public. You will also regularly interact with other members of staff and people from other organisations.

Communication is the sending and receiving of signals. It is all about passing your thoughts or ideas to another person. The 'sender' decides what thoughts they wish to pass on, 'encodes' those thoughts into the most effective form of communication and then 'sends' those thoughts to the 'receiver'.



The different types of communication

Verbal communication is the use of words and tone to convey a message when interacting with another person. The words you use are important, but so is the tone you use to express those words. It's not just what you say, but how you say it that counts. Verbal communication includes:

- speaking
- listening
- reading (aloud)
- pitch and tone of voice

Non-verbal communication is everything else that you do when you communicate with another person on a face-to-face basis. Non-verbal communication includes:

- gestures
- stance
- eye contact
- facial expression

Written communication is the sending of messages in the form of letters, emails, memos, pictures, symbols, script, text messages, etc.

The importance of effective communication

When working as a security operative, using effective communication skills will not only help you to successfully get the job done, but it will also ensure that people receive a good impression of you.

To effectively communicate in the workplace, you will need to:

- choose an appropriate medium and use appropriate language for the message and recipient it is intended for
- deliver the message clearly
- check the recipient's understanding of the message, for example by asking them to repeat the message back to you

It is important to use effective communication whether dealing with internal or external customers in the workplace.

When used internally, it will promote effective teamwork that will help you and your colleagues to provide an effective service to customers, in turn positively promoting your organisation as a professional establishment.

Communicating effectively will also help to prevent misunderstandings which could lead to mistakes being made and therefore can help to reduce incidents of conflict, aggression or even violence.

Chapter 7: How to communicate effectively as a security operative

Effective communication in a team

Communication skills play an important role in how you interact with your colleagues, supervisors and managers. You should treat all members of staff with courtesy and respect and you should expect to be treated in the same way.

Good teamwork in the workplace:

- promotes safety
- provides a professional and safe service and establishment
- supports colleagues
- promotes efficiency

Diverse customer needs and expectations

All customers are different people with differing needs and expectations. They may come from different countries, have different faiths or religions, or they may just be from a different age group. Customers may also have different levels of physical or mental ability.

People form their own personal values as they grow up. Where they were born, where they live, how they were brought up, their friends and family, their jobs – all of these factors go towards forming a person's values.

As a security operative, you need to take into account other people's values, and try to choose the most appropriate and effective way of dealing with them. For example, you would speak to a distressed young child in the street very differently to how you would treat a drunk, aggressive customer outside a pub. Both are customers if you have to deal with them as part of your duties, but both would need to be dealt with differently because of their different values, needs and expectations.

Customers with particular needs

It is important to acknowledge and respect individuals with particular needs. You may need to consider adapting how you would normally communicate with individuals e.g. shouting at a visually impaired person will not help them understand you. Particular needs may include physical disabilities, learning difficulties, sensory impairment, English as a second language or being under the influence of drugs and/or alcohol. You may need to speak slower than usual when giving information, assistance or directions or draw a picture to provide guidance.

The principles of customer service

One of your main roles as a security operative is looking after people. How you treat people when you deal with them is very important. Customer care is all about how you deliver your service and how you provide security to your customers on a day-to-day basis.

Examples of how you can deliver good customer care include:

- being professional with every customer
- being approachable
- communicating with them effectively
- acknowledging them
- concerning yourself with customers' needs
- building a rapport
- treating customers as you would wish to be treated yourself
- going out of your way to help customers
- leaving customers pleased with how you have dealt with them

Dealing with problems

Good customer service can often avoid problems occurring. However, some problems may not be caused by you and may be out of your immediate control. In these circumstances you must do everything within your power to appease the customer:

- acknowledge and listen to the customer
- establish the customer's need
- put yourself in the customer's position
- accept responsibility for the problem
- involve the customer in the proposed solution
- see it through, make sure any promised actions are carried out.

Different types of customer

As a security operative, you must understand that every single person you come into contact with is a customer. In your role, you will be providing customer service to both internal and external customers (direct and indirect).

Internal customers

Internally (within your own company), your customers include your work colleagues, supervisors, managers and anyone working for any other company or organisation on the site.

External customers (direct and indirect customers)

External customers are any other customers you may come into contact with, including visitors to the site, workmen, delivery drivers, the emergency services, neighbours and members of the public.

LETTERS

A	Alpha	**N**	November
B	Bravo	**O**	Oscar
C	Charlie	**P**	Papa
D	Delta	**Q**	Quebec
E	Echo	**R**	Romeo
F	Foxtrot	**S**	Sierra
G	Golf	**T**	Tango
H	Hotel	**U**	Uniform
I	India	**V**	Victor
J	Juliet	**W**	Whiskey
K	Kilo	**X**	X-ray
L	Lima	**Y**	Yankee
M	Mike	**Z**	Zulu

The phonetic alphabet

The NATO phonetic alphabet was developed in the 1950s to be intelligible and pronounceable to all NATO allies in the heat of battle. It is now widely used in business and telecommunications in Europe and the rest of the world. The phonetic alphabet requires words to be spelt out by their letters during a conversation. All the letters sound different, so there is no confusion about what people are saying.

You may need to use the phonetic alphabet during the course of your duties as a security operative, as you may well have to use the telephone or radio to communicate with other members of staff, outside organisations or members of the public. It is important that this is always done professionally and politely - always remember to use clear language.

Effective telephone/radio communication between security teams and other people on-site is essential and helps to deal with incidents swiftly and efficiently.

1 Provide THREE examples of verbal and non-verbal communication.

Verbal	Non-verbal

2 Give THREE examples of good customer service.

1

2

3

3 State the importance of effective communication in the workplace.

Chapter 8: Record-keeping relevant to the role of the security operative

Accurate record-keeping

It is important that accurate records are documented and kept for any incident or accident that happens when you are on duty as a security operative. By keeping accurate records, you will be:

- complying with the law
- providing a clear audit trail of the incident or accident
- preventing yourself from having to rely on your memory

Reporting and recording procedures

During the course of your normal duties as a security operative, you may have to deal with a variety of events. You may also have to become involved in serious incidents or be called to the scene of a crime. The site or venue's policies will give details of what to do and who to inform when serious incidents occur or when crimes are committed, and these must be followed.

Serious incidents like injuries, fires or bomb threats will all require the assistance of the emergency services. You must know how to inform them and be able to provide them with as much information about the incident as possible, so that the appropriate help can be sent to deal with it. Crimes, arrests, serious disorder and incidents taking place outside of the premises will normally mean that the police have to be called.

Using notebooks

While full incident reports can be completed in the relative comfort of an office or staffroom, there are occasions when you may need to make accurate, timely notes while working at the scene of an incident. To ensure that sufficient details about a routine or unusual event are taken at the time, you will often need to use notebooks. A fuller report can be made of the incident later, using the information in the notebook taken at the time.

Security notebooks are still official documents, however, should be used properly at all times. They should only be used to record work-related matters. For these reasons, notebooks should be kept securely as they may contain confidential information about the venue, the client, the security company or operational procedures.

Remember, your notebook may need to be produced and used as evidence in court.

Notebooks need to be completed in black ink and notebook rules should apply. The mnemonic **'NO ELBOWS'** is a useful way of understanding and remembering the general rules for when using notebooks.

NO	**E**rasers
NO	**L**eaves (pages) **t**orn **o**ut
NO	**B**lank spaces
NO	**O**verwriting
NO	**W**riting between the lines
AND	**S**tatements in direct speech

Notebooks should be used to record both routine and unusual events. As well as recording day-to-day information like duty or shift times, they should also be used at incidents or during emergencies to record descriptions, names and addresses of witnesses, vehicle registration numbers and timings.

Chapter 8: Record-keeping relevant to the role of the security operative

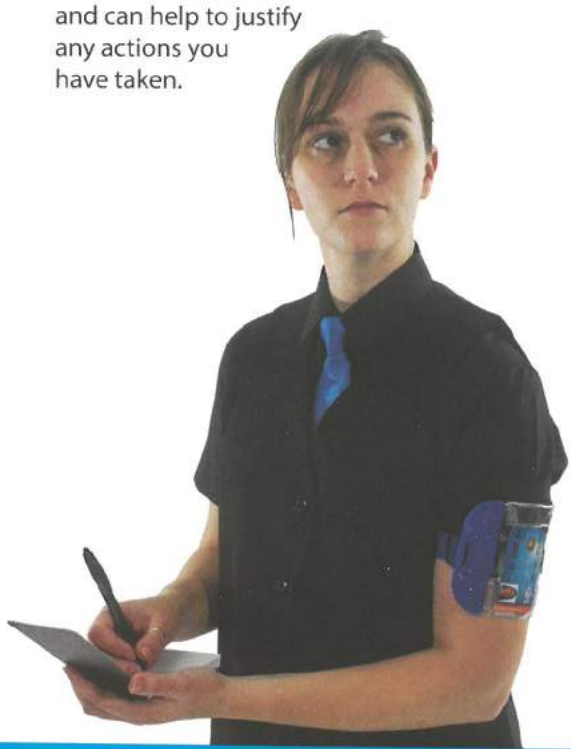
Types of records to be completed

Notebooks should only ever be used to record workplace information, and never to record personal information or reminders. Other documents used to records details might include:

- incident records
- accident records
- searches and checks
- logbooks
- pocket notebooks
- search/visitor/key registers
- duty sheets
- accident reports
- lost/found property registers
- message books
- handover reports
- other site-specific reports

As a security operative, you need to ensure that you know what records you are required to use at the venue, where they are kept and how to complete them.

These various reports provide a permanent written record of incidents that have happened and can be used to refresh your memory prior to giving evidence in court. They can also be used to assist the site/venue to comply with the law, assist outside agencies, protect you from malicious allegations and can help to justify any actions you have taken.



Incident reports will need to show:

- **the day, date and time of the incident**
- **what happened**
- **how it happened**
- **where it happened**
- **how you were alerted to it**
- **what you saw**
- **what you were told**
- **what action you took**
- **what the result was**
- **details of any witnesses**
- **any descriptions of people or property**

Records need to be completed as soon as possible following the incident.

Remember to include who the report is for and who wrote it.

They should be purely factual, without personal opinion, and each separate report should be signed, dated and timed.

HOW

WHAT

WHERE

WHEN

WHY

WHO

REMEMBER

A ACCURATE

B BRIEF

C CLEAR

Reports should be **accurate**, **brief** and **clear**.

Recording information

Security operatives must record as much information about the incident or crime as they can at the time it occurs, so that a proper report can be made once the matter has been dealt with. A notebook is the ideal place to record such details at the scene. This information can be put into a formal incident log later if required.

Typical incidents that would require recording properly include:

- entry refusals
- incidents of trespass
- the use of force
- arrests
- serious crime
- accidents
- searches
- seizures of drugs, weapons or other items
- disputes and complaints
- suspicious behaviour
- visits by police or other authorities/agencies
- all other emergencies

Statements

A statement is a written account of what evidence a witness can give about an incident. The rules about statement writing and giving evidence can be found in the Police and Criminal Evidence Act (PACE) 1984. Formal police statements are often referred to as 'Section 9 statements'. You may also wish to refer to the Criminal Justice Act 1967 section 9 for proof by written statement'.

NI

The Police and Criminal Evidence (Northern Ireland) Order 1989.

Should you witness an offence, arrest someone for committing one, or in any other way become involved in an incident to which the police are called, you may be required to make a statement giving details of your involvement.

Statements handwritten on official police statement forms give a chronological description of a sequence of evets as seen by a witness. They describe and identify persons, scenes and events, give details of actual words spoken by various parties, and either prove or disprove matters in issue. Statements are taken for the following reasons:

1. To allow police officers to collate and evaluate evidence during investigations
2. To record witnesses' evidence as soon as is practicable after an incident
3. To submit as evidence (when not contested) in court to save the attendance of a witness
4. To refresh a witness's memory prior to actually giving evidence in court

If you are required to make a statement, the police will help you. They will ask you questions about the incident before writing your account down in a manner which is acceptable to the courts. You are entitled to write your own statement if you wish to, but this is not recommended. There is a declaration at the top of the statement from which reads:

'This statement (consisting of... pages each signed by me) is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have wilfully stated anything which I know to be false or do not believe to be true'.

It is a serious offence under common law to commit an act which shows a tendency and is intended to pervert the administration of justice, and this includes the fabrication of false evidence, even it if never used.

Having written the statement, you will be asked to sign the declaration at the beginning, sign the bottom of each page and after the very last word. The statement can then be tendered as the evidence you are able to give about the incident at any subsequent court proceedings.

Use of force in statements

If you are required to make a formal written statement to police about any force you have had to use against a person, or have to explain any force you have used while effecting a lawful arrest, then the following details need to be included:

- time, date and place of incident
- how you were called to the incident
- what type of incident it was
- whether you were alone or with other supervisors
- how you approached the incident
- what you saw and heard
- how many people were involved
- the person's attitude and state of mind
- the person's size compared to yours, details of any weapons
- how you felt about the situation, e.g. frightened, in fear of being assaulted etc.
- the actions you took
- what you said to the person
- what the person said in return and how he reacted
- why you decided to use force
- how much force you used
- what the person's level of resistance was
- how you restrained or ejected the person

- how the person was held until the arrival of police
- details of any injuries you or the other person sustained
- details of the officer who took the person from you
- details of any witnesses to the incident
- details of first aid and/or medical support provided
- details of admission to hospital
- details of the support involved and any follow-up action required

Identification in statements

Should you be required to describe a person you have seen in a statement, as well as giving as complete and accurate a description as you can, you should also cover the following points:

- how long you observed the person for
- how far the person was away from you
- what the lighting conditions were at the time
- whether your view of the person was impeded in any way
- whether you have ever seen the person before and if so, how many times
- whether you had any special reason for remembering the person
- if you subsequently identified the person to police, how much time passed between originally seeing him and the identification
- any differences between your descriptions of the person and how they looked when you identified them to the police

Covering these points in your statement provides good evidence for the prosecution where the case depends on the identification of the accused and shows a professional understanding of both the rules of evidence and the importance of proper descriptions and identification.

Attending court

Before attending court, you should take the opportunity to refresh your memory by reading your incident report/notebook.

Attending court can be a stressful experience and the courts have a witness support system that can assist with the process of preparing yourself before giving evidence in court. The following sets out what can be expected:

- arrive at court in good time, let CPS know you are a witness and follow any advice given
- read your statement (if not already read through)
- when called into court, stand in the witness box. If you have a faith you will be asked to take an oath; if Christian, you will have to hold a bible and read the oath:
  - 'I swear by almighty God that the evidence I give, shall be the truth, the whole truth and nothing but the truth'
- there are different books for each religion, for example, the Koran for Islam, but if the witness does not wish to take an oath (they may be agnostic), they can take an affirmation as follows:
  - 'I do solemnly, sincerely and truly declare and affirm that the evidence I shall give shall be the truth, the whole truth and nothing but the truth'
- you will be asked questions by the solicitors (barristers in the Crown Court) but you should address your answers to the magistrate or jury, as they will be considering your evidence
- try and keep your answers straightforward and avoid trying to embellish your statement; if you do not know the answer to a question, don't be afraid to say so
- avoid giving opinion (unless asked) or making assumptions; your job is to report the facts of what you saw and did
- you must follow your organisation's policies and procedure when attending court

1 Explain the importance of accurate record-keeping.

2 Identify the types of information that should be included in records.

1

2

3

4

5

6

3 Describe the process of attending court to give evidence.

Chapter 9: 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

Chapter 9: 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.

Chapter 9: 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.

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

Public sector counterterrorism experts:

Centre for the protection of National Infrastructure (**CPNI**)
www.cpni.gov.uk/cpni-context

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.

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

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

T **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).

- 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 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

Chapter 9: 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 manger 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**.

1 What are the FIVE different threat levels?

1

2

3

4

5

2 What are the most common terror attack methods?

3 Identify behaviours that could indicate suspicious activity and explain how you would respond to the activity you have identified.

Chapter 10: Keeping 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, report as soon as possible to your supervisor, the police or call Crimestoppers.

Chapter 10: Keeping 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

1 Identify FIVE factors that could make someone vulnerable.

1

2

3

4

5

2 Identify behaviours that may be exhibited by sexual predators.

3 Identify indicators of abuse.

1

2

3

4

Chapter 11: Good practice for post incident management

Accessing help and support

Because of their varying degrees of experience and exposure to conflict, people cope with assaults and incidents in different ways.

Incidents where you are abused, threatened or even assaulted in the workplace can have various different impacts on everyone and so you need to be aware of what is available out there to help you if you need assistance or support following a traumatic incident.

It is important, therefore, that businesses and organisations are able to help staff after an incident of workplace violence, particularly in relation to:

- providing immediate and ongoing support
- helping all members of staff to learn from the incident
- updating policies and procedures to improve safety
- sharing good practice

Typical effects

Anyone could show any or even all of the following short-term or long-term symptoms following exposure to workplace violence:

- sickness
- insomnia
- behavioural changes
- becoming withdrawn
- anxiety
- intolerance
- hypersensitivity
- fear
- depression
- loss of confidence
- stress
- post-traumatic stress disorder (PTSD)

Responses to incidents

Typical symptoms are how the brain and body react to abnormal situations or incidents. The severity of the symptoms will usually depend on the severity of the incident, although something that might not affect you could well affect one of your colleagues and vice versa.

Certainly, in the time directly following an incident, anyone could start to feel shock, anger, embarrassment and disbelief that this has actually happened to them at all.

Post-incident support

It is vital that if a member of staff starts to show any signs that they may be suffering from any of these symptoms, support must be given immediately to reduce the changes of long term effects. Support can be provided by:

- colleagues
- management
- counsellors
- helplines (such as the Samaritans)
- citizens advice
- trade unions
- trade publications such as victim support: **(www.victimsupport.org.uk/)**
- the internet

Professional medical help may be even required for serious problems.

Chapter 11: Good practice for post incident management

Reflecting on and learning from conflict

Dealing with people, particularly within the private security industry, is a large ongoing learning curve. You never stop learning, and there is always room for improvement in everything you do. This is especially true when it comes to how you deal with conflict, anger, aggression and violence.

There are 6 basic steps to take following an incident.

1 STEP 1 - Reflect on what happened

Consider: *What happened?* *Why did it happen?* *What went wrong?* *What could we have done better?*

2 STEP 2 - Recognise trends and any poor practice

Consider: *Does this problem occur regularly?* *At any particular place or time?* *Can we reduce or stop these types of incidents?* *Is there something we are doing wrong?*

3 STEP 3 - Share good practice

Consider: *Did we do something well?* *Does everyone know how to do it?* *Is extra training required?* *Does it need to be a policy?*

4 STEP 4 - Learn from what happened

Consider: *How do we make sure this doesn't happen again?* *Can we improve something for next time?*

5 STEP 5 - Update policies, practices and procedures

Consider: *Are our policies, practices and procedures up to date?* *Can anything be added or improved?*

6 STEP 6 - Monitor progress

Consider: *How can we record future incidents better?* *How can we monitor the effectiveness of any changes made?* *When and how do we re-evaluate our future performance?*

The proper debriefing of these types of incidents can help you to improve how you deal with similar problems in the future. Organisations can use data that has been collected for licensing hearings and they may even be able to reduce the chances of them happening in the first place, or even stop them from happening at all. And if they do occur, you should be able to provide an agreed, common positive response each time, automatically improving your own safety, as well as the

safety of customers, colleagues, other members of staff and the public. All members of the security team, particularly those involved in the original incident, should take part in this process so that they can help to make the changes required to deal with future conflict situations more effectively.

Improving practice

Like all industries, the security industry needs to continue to evolve and progress. As a security operative you have the responsibility to ensure that you continually contribute to improving practices within the industry.

Improved practices help to:

- promote a professional service
- increase safety for staff
- promote teamwork
- increase safety for customers
- identifies procedures or methods to better deal with situations effectively

1 Explain where post-incident support or resources can be found.

2 Explain why it is important to access support following an incident.

Key tasks

3 Identify FIVE benefits of reflecting on an incident.

1

2

3

4

5