

1. Main characteristics of the private security industry

Industry Employs over 500,000 people from technology to uniformed security services, working with the public and private sectors.

Purpose **Deter, prevent and detect crime.** **Deterrents** include: Visible security such as uniformed security staff, CCTV and alarms.

Prevention is taking precautions to reduce the risk of crime. Actions include: Checking windows, security lighting, fences and doors • Effective access control • Controlling the issue of keys • Ensuring procedures are followed • Responding to changes in the environment and suspicious activity • Monitoring electronic article surveillance points.

Detection includes: Identifying and reporting signs of criminal activity • Identifying suspect behaviour • Apprehending criminals • Controlling security crime scenes.

Prevent and reduce loss, waste and damage including fire, flood, poor storage, abuse of facilities, equipment or materials. This is done by: Deterring actions that could lead to loss or damage • Removing and reporting causes of damage • Monitoring the environment for things that might increase risk • Responding to incidents and educating people in correct behaviour.

Monitor, reduce and respond to safety risks to employees, customers, visitors or the general public.

Monitoring activities including: Checking safety critical systems • Ensuring compliance with safety procedures • Observing people to ensure that they are acting in a safe manner • Reporting objects and activities that are unsafe.

Reducing risk by: Eliminate risks • Alert others to hazards and risks • Ensure that emergency exits and escape routes are clear.

Responding by: Providing or coordinating first aid • Controlling the scene and coordinating responses • Making sure accidents and injuries are reported and recorded • Managing traffic and keeping emergency routes open.

Assisting with recovery activities, which could include: Securing the premises after a break in • Helping to bring an area back to operation • Ensuring safety equipment is operational after use • Adjusting routines to respond to breaches in security • Reporting on casualties/incidents to the Human resource department.

Sector and career opportunities Includes door supervision, security guarding, protecting cash and valuables in transit, vehicle escorts, monitoring CCTV, prison and prison escort duties, close protection, vehicle clamping and immobilisation, private investigation, consultancy, monitoring and response. These range across the sectors of retail security, transport security, leisure security. It also includes technology sectors such as the design and installation of intruder alarms, CCTV and access control systems, IT security and product marking.

The industry provides careers in operations, training, personnel, finance and general management. The career route for a security operative such as a guard would be security guard → team leader → site or area supervisor → operations management, training, human resources, consultancy or sales.

Functions the SIA of The private security industry is regulated by the **Private Security Industry Act 2001**, which covers England and Wales, and was extended to include Scotland in 2005 and Northern Ireland in 2009. The purpose of the Act was to: Raise standards • Remove criminal elements from the industry • Increase public confidence and safety • Establish the SIA and licensing.

SIA responsibilities: Compulsory licensing of certain jobs in the security industry • Management of the voluntary Approved Contractors Scheme • Sets and approves standards of conduct, training and supervision • Monitors the performance of the private security industry and the Private Security Industry Act • Undertakes inspection and enforces regulation.

Activities included in the scope of regulation are manned guarding services provided under contract (cash and valuables in transit, close protection, public space CCTV surveillance, security guarding); door supervision (in-house and contract); and key holding provided under contract. The Act also allows private investigators and security consultants to be licensed but as yet, these are not licensable activities. Vehicle immobilisation used to be a licensable activity, but has since been outlawed on private land in England and Wales.

Types of licence: There are two types, frontline and non-frontline. Frontline are for those in an operational role such as security officers, door supervisors and CCTV operators and require training and Criminal Record Bureau (CRB) checks. Non-frontline licences are for managers and support staff not directly involved in operational duties and these also requires a CRB check. Licences are valid for three years but can be cancelled by the SIA for malpractice or bad behaviour.

Those requiring a licence include all directors, managers and staff of contract security firms • Agency workers performing licensable duties • Managers and supervisors working with security operatives supplied under contract including agency managers/supervisors • In house and contract door supervisors.

Penalties for failing to possess a licence are a fine of up to £5000 and or a prison sentence of up to 6 months for individuals. Penalties are also applied to the employing company.

The Approved Contractors Scheme is not mandatory for companies. To be approved a company must show that a percentage of deployed staff hold an SIA licence, all directors are considered fit and proper persons and hold a valid SIA licence, there are no significant complaints about the organisation and that the company has adopted certain quality standards and have been assessed against those standards. Assessment for ACS is undertaken by a body approved by the SIA such as the NSI, SSAIB or BSI.

Who's who

In addition to the SIA, there are other organisations with influence in the industry. The **British Standards Institute (BSI)** sets technical and operational standards. These standards are voluntary and include BS7858 code of practice on screening of personnel employed in the security industry, BS7960 code of practice for door supervisors/stewards, BS7984 code of practice for key holding and response services. **Inspectorate** organisations, which inspect companies against voluntary standards such as ISO 9000 quality standards and industry technical and operational standards. They also function as inspectorate bodies for the ACS scheme. The two main inspectorate bodies in the industry are the National Security Inspectorate (NSI) and SSAIB.

Trade and professional bodies who are responsible for representing their members and include the International Professional Security Association (IPSA), British Parking Association (BPA), The Security Institute (TSI) and the British Security Industry Association (BSIA). **Training** is delivered to the standards agreed by the SIA with qualification regulators, certificated by awarding organisations such as Edexcel and IQ, and trained by trainers approved by an awarding organisation, often using materials supplied by an organisation such as SAFE. Higher level training and education is also available, often against standards developed by the industries Sector Skills Body, Skills for Security.

Qualities and skills

and Security staff should: Be of smart appearance • Courteous and polite • Honest and trustworthy • Alert with good observational skills • Have good verbal and written communication skills • Work to procedures and instructions • Willing to take responsibility for and solve problems as they arise • Confident and deal with difficult people in an assertive manner • Reliable and able to work with integrity • Able to relate to a wide range of people • Be non judgmental in their approach to people • Able to work independently or part of a team • Be patient in dealing with people and situations • Able to prioritise needs and responses to situations • Calm and respond quickly to emergencies and difficult situations • Discrete and tactful, maintain confidentiality • Non-confrontational • Have a basic understanding or willingness to work with IT.

Crime reduction initiatives

National and Local Pubwatch initiatives, where intelligence is shared between licensed premises • Crimestoppers, (a crime fighting charity) • Schemes to share intelligence in the retail sector using radio link or mobile telephony. • Local police initiatives • The police and authorities also co-operate with stakeholders on issues relating to terrorism, (eg Project Griffin and Project Argus) • Police initiatives relating to major events where activities need to be co-ordinated across a range of partners • Red and Yellow card schemes, where security staff are able to issue red or yellow cards in the same way as they are used in football.

Benefits of should include; Reducing the opportunities for crime and disorder to take place, Improves security of vulnerable targets, reduces crime and disorder and improves safety in the general environment, removes the means to commit crime, increases knowledge and intelligence to support monitoring activities, reduces risks of crime and disorder on your customers site/venue.

2. Legislation that is relevant to people carrying out a licensable activity

Types of law

Civil law is also known as private law in Scotland, and involves non-criminal cases and enables individuals or organisations to take action against each other in order to settle disputes. Civil cases do not result in prison sentences or fines. If a case is proven, the result is normally compensation or the division of assets. The burden of proof is lower than in criminal cases. Examples of civil cases include disputes about property, employment, libel/slander, consumer issues, and commercial issues. Security personnel **do not have any powers of arrest for a civil dispute.**

Criminal law is the means by which the government identifies and criminalises behaviour that is considered wrong, damaging to individuals or to society as a whole or is otherwise unacceptable. Cases are usually brought on behalf of the state against an individual accused of committing a criminal offence by the Crown Prosecution Service in England and Wales, or The Procurator Fiscal in Scotland. Only the state can bring a criminal case to court, and the state must prove beyond reasonable doubt that the person accused of the crime is guilty. Punishments for committing criminal offences include a prison sentence, fine, probation and community service. Security staff in England and Wales have the same power of arrest as members of the public for indictable offences.

In Scotland, criminal law forms part of public law. Security staff can make arrests for an offence at common law, but **cannot** affect arrests for statutory offences.

Although the law allows citizens to make arrests it should only be used as a last resort.

The burden of proof in a civil case is considered against ‘a balance of probabilities.’ The burden of proof for a criminal case is higher, and has to be ‘beyond reasonable doubt.’ This means that the evidence must leave no doubt that the crime took place and was committed by the accused. In Scottish law, there is a requirement for evidence of proof to be backed up (corroborated) by at least one other source of evidence.

Statute Law are written laws that are passed by Acts of Parliament (known as statutes). **Common Law** is non-codified legislation handed down and developed by courts over the years.

Private Security Act

The aim of the act when it was passed into law was to: Raise standards in the private security industry • Increase public confidence in the private security industry • Increase public safety • Remove criminal elements from the private security industry. The act paved the way for the industry to access criminal records. • Establish the SIA • Establish Licensing.

Equality

The Equality Act 2010 was designed to provide a single piece of legislation dealing with equality. The Act affects employers, in relation to employment practices, service providers in relation to the way they deal with customers and a variety of other groups including the public sector. It makes discrimination, harassment and victimisation illegal for certain protected characteristics. Not all of the illegal acts apply to every protected characteristic.

Types of discrimination

Direct
Where a person is treated less favourably than another person because of a protected characteristic.

Associative
Direct discrimination against someone because they associate with another person who possesses a protected characteristic.

By perception
Direct discrimination against someone because the other person thinks that they possess a particular protected characteristic.

Indirect
Can occur when there is a rule or policy that applies to everyone but disadvantages a person or group that possess a particular protected characteristic.

Harassment is a type of indirect discrimination where the victim can show that the behaviour caused injury to feelings. It can be defined as ‘Unwanted conduct that violates dignity or creates an intimidating, degrading, or humiliating environment.’ **Examples of harassment** depend on the protected characteristic, but offending behaviours can include innuendoes, comments and remarks, insensitive jokes, inappropriate e-mails or text messages, inappropriate actions. For instance sexual harassment could include sexual innuendoes, lewd comments sexually suggestive remarks, requests for sexual favours, insensitive jokes,

touching and fondling, unwelcome sexual advances, the display of sexually orientated materials.

Perception of harassment: Whether the action was intended to cause offence or not does not matter – if the employee being subjected to the behaviour finds it unacceptable and they feel damaged or harmed by it, this constitutes potential harassment. Harassment is normally characterised by more than one incident of unacceptable behaviour, but in some circumstances just one instance may constitute harassment if it is sufficiently serious.

Third party harassment: The Equality Act makes employers potentially liable for harassment of their employees by people who are not employees of the company such as customers or clients. It applies to the following protected characteristics (sex, age, disability, gender reassignment, race, religion or belief and sexual orientation) where the employer has failed to take reasonable steps to prevent it.

Victimisation: Victimisation occurs when an employee is treated badly because they have made or supported a complaint or raised a grievance under the Equality Act, or because they are suspected of doing so. An employee however, is not protected if they have maliciously made or supported an untrue complaint.

Protected characteristics

Discrimination affecting Protected Characteristics in the workplace and where goods and services are provided. Services include training, hairdressing, libraries, etc.

<ul style="list-style-type: none"> ● Provision of goods/services and in the workplace ○ Workplace only 	Age	Disability	Gender reassignment	Race	Religion or belief	Gender	Sexual orientation	Marriage & civil partnership	Pregnancy and maternity
Direct Discrimination	○	●	●	●	●	●	●	○	●
Associative Discrimination	○	●	●	●	●	●	●		
Discrimination by Perception	○	●	●	●	●	●	●		
Indirect Discrimination	○	●	●	●	●	●	●	○	
Harassment	○	●	●	●	○	●	○		
Harassment by a Third Party	○	●	●	●	○	●	○		
Victimisation	○	●	●	●	●	●	●	○	●

Age The Act applies to people of all ages, but different treatment because of age is lawful if it can be justified. Age is the only protected characteristic that allows employers to justify direct discrimination.

Disability A person is disabled if they have a physical or mental impairment that has a substantial and long-term effect on their ability to carry out normal day-to-day activities. Employers must Make reasonable adjustments to allow staff to overcome any disadvantage because of the disability - Not treat the disabled person unfavourably because of something connected with their disability - Not indirectly discriminate against disabled people by applying a general rule that disadvantages an employee or job applicant with a particular type of disability.

Gender reassignment The Act protects transsexual people. The Act does not require a person to be under medical supervision to qualify as a transsexual and those living permanently as a member of the opposite sex, but have not undergone medical procedures are protected by the Act. Transvestites (cross dressers) are not transsexual as they do not intend to live permanently as a member of the opposite sex.

Race For the purpose of the Act, race includes colour, nationality and ethnic or national origins.

Religion or belief This includes any religion, or any lack of religion. Employees and job seekers are protected if they do not follow a certain religion or have no religious beliefs at all. Belief means any religious or philosophical belief or a lack of a belief. Under the legislation, mainstream religions, and religious sects are protected as they are religions.

Gender Both men and women are protected under the Act.

Sexual orientation The Act protects bisexual, gay heterosexual and lesbian people.

Marriage and civil partnership The Act protects employees who are married or in a civil partnership against direct and indirect discrimination in the workplace.

Pregnancy and maternity A woman is protected against discrimination on the grounds of pregnancy and maternity during the period of her pregnancy and any statutory maternity leave to which she is entitled.

Equal opportunities legislation impacts upon a range of employment policies, including those affecting: Recruitment; Access to training; Pay and benefits; Promotion opportunities; Terms and conditions; redundancy; Dismissal.

Provision of services People who access goods, facilities and services are protected from direct discrimination on the basis of a 'protected characteristic'. The relevant characteristics are disability, gender reassignment, pregnancy and maternity, race which includes ethnic or national origins, colour and nationality, religion or belief (but not currently from harassment), gender; sexual orientation (but not currently from harassment). Except in the case of pregnancy and maternity, people who are protected do not actually have to possess the characteristic themselves. Protection also applies, for example, where the person is unfairly treated because they are wrongly thought to have the characteristic or because they associate with someone who has the characteristic.

Disabled people must not be treated less favourably than others because they are disabled. Businesses must make reasonable adjustments to help disabled people access their goods, facilities and services.

As a matter of good practice and good business, everyone accessing your employer's goods, facilities or services, or those of the client, should be treated fairly, regardless of their age, gender, race, sexual orientation, disability, gender reassignment, religion or belief, and guard against making assumptions about the characteristics of individuals.

Reasonable adjustments

There is a requirement for both employers and providers of goods and services to make reasonable adjustments to accommodate people with disabilities in order to help overcome the practical effects of their disabilities. This obliges employers to consider removing the disadvantage caused by the nature of any individual disability both job applicants, employees and customers.

They apply where any arrangements made by the employer, or any physical feature of the premises, place a disabled employee or disabled job applicant at a substantial disadvantage. Unjustified failure to make reasonable adjustments is unlawful discrimination.

N.B. There is no general duty to make adjustments in anticipation of employing a disabled person.

Adjustments can be made to working arrangements to prevent disadvantage to employees or job applicants these include:

- If an employee's condition means that they cannot drive, allocating their driver duties to another employee if they form a minor part of the job.
- Relocating a person with limited mobility to the ground floor or moving a disabled employee to other premises if the usual place of work is inaccessible.
- Acquiring a specially adapted keyboard for someone with arthritis in their hands or for someone with a visual impairment.
- Providing special telephone equipment for an employee with a hearing impairment.

3. Safe working practices to comply with legal requirements

Importance of health and safety Organisations have a legal responsibility defined in a wide range of health and safety regulations, which have been designed to make the workplace a safer place. Failure to comply can lead to prosecution or even closure of a business. However, health and safety is also about creating a more efficient workplace by reducing time lost to accidents and poor health, reducing risk to employees, and maintaining the reputation of the business.

Cost of accidents Where accidents or injuries happen, they come at a cost to both the business and the individual concerned. **Personal costs** include:

- Loss of income
- Pain and suffering
- Loss of mobility
- Stress
- Inconvenience
- Disability or death

Costs to the business might include:

- Increased insurance premiums
- Compensation claims
- Legal costs
- Damage to facilities
- Damage to company reputation
- Fines
- Sick pay / increased overtime payments
- Lost time / additional work

Compliance with legislation The Health and Safety at Work Act is the most significant act relating to UK health and safety legislation, but there are other related Acts that are important. The Health and Safety Executive (HSE) is responsible for co-ordinating and leading legislative developments on health and safety issues in the UK. Compliance with health and safety legislation is a legal requirement and failure to do so can lead to imprisonment or other penalties imposed.

Health and safety inspectors can enter work premises at any time. Usually the inspector will be visiting to undertake a health and safety inspection. They could also visit after an accident or as a result of a complaint. If the visit is the follow up to an accident → the inspector will be seeking to investigate the causes → provide advice on any action that might be taken to stop similar accidents happening again, or → assess whether there has been a breach of health and safety law.

If an inspector considers that an organisation is breaking health and safety law, or its activities give rise to a serious risk, they might issue an informal warning (verbally or in writing). They can also take a more formal approach and issue an improvement notice or prohibition notice. An improvement notice gives the employer a defined period of time in which the improvement to working practices, procedures or equipment must be made. A prohibition requires the activity, practice or process to stop immediately until the improvement is made. A prohibition notice can affect a part of the operation, or have the affect of closing the whole operation until the improvements are made. Inspectors also have the power to prosecute the company or individuals.

Responsibilities under legislation The Health and Safety at Work Act sets out the general duties that employers have towards employees and members of the public, and employees have to themselves and each other. The Act applies to employers, employees, visitors and customers, contractors, suppliers, end users, anyone that enters the site legally and anyone entering the site illegally. **WE ALL HAVE A COMMON DUTY OF CARE.**

Duty of employers The employer's duty is to make the workplace safe without risk to health as far as is reasonably practicable.

Procedures	<ul style="list-style-type: none"> • Ensuring that safe systems of work and procedures (including emergency procedures) are set. This includes evacuation procedures, and that storage, movement and usage of hazardous substances. • Monitor to ensure that safe practices on safety critical procedures are followed, e.g. Substance abuse testing of company vehicle drivers and crane operators.
Facilities	<ul style="list-style-type: none"> • Ensure that plant, machinery and equipment is safe, suitable for intended use and well maintained. • Provide free any protective clothing or equipment where the risks cannot be adequately controlled by other means. • Provide adequate first aid facilities that are maintained properly.

	<ul style="list-style-type: none"> • Provide adequate welfare facilities this includes toilets facilities, drinking water, etc.
Reporting	<ul style="list-style-type: none"> • Report certain injuries and dangerous occurrences (RIDDOR) which is covered in more detail towards the end of this lesson.
Risk assessment	<ul style="list-style-type: none"> • Identify any hazards present. • Precautions should be taken against flammable or explosive hazards, electrical equipment, noise and radiation. • Evaluate the risks in relation to that hazard. • Identify preventative and precautionary measures. • Record significant findings. • Review the significant findings.
Fostering good health and safety culture / training	<ul style="list-style-type: none"> • Involve the workforce in developing health and safety culture. • Appoint a competent person to assist in health and safety responsibilities. • Give information, instruction, training and supervision necessary for health and safety of employees (including regular refresher courses).

If an employer employs 5 or more people, they must assess the risks, recording the findings of the assessment (Health and Safety at Work Regulation 1999) and draw up a health and safety policy statement.

Duty of an employee and the self-employed The duties of an employee, which also applies to self-employed people and agency staff, are to take reasonable care for their own health and safety and that of others who might be affected by what they do. Clearly, this would include anybody entering the site that might be affected by their actions. They must also co-operate with employers and others in order that they can discharge their legal duties.

Employees must only carry out work related tasks they are trained in and to carry out these tasks in accordance with the training received • Operate equipment safely- comply with operating instructions and do not misuse equipment • Follow H&S procedures - wear protective clothing, follow safety signage • Cooperate with and participate in employer provided training • Report faults and defects found on machinery or equipment as soon as they occur • Report injuries and accidents to employers.

It should be recognised that it is not just what you do that is important it is also what you do not do. These are known as your acts and omissions within health & safety legislation and you can be prosecuted, if found negligent in either.

In the security industry exercising your duty of care will include such things as: • Deciding the need and recognising the consequences of physical intervention • Making sure that you are trained to take on the role or the job • aspects of Taking action on safety issues observed on site.

Duty of a visitor a Visitors are expected to: Follow instructions detailed in pre-visit instructions or those given on entry to the site • Refrain from entering unauthorised areas • Not misuse equipment provided for the purpose of health and safety • Carry out instructions detailed on health and safety signage • Wear protective clothing provided to them for the purpose of the visit • Park vehicles in allocated spaces provided • Comply with fire and evacuation policies and procedures.

Duty of a Contractor Contractors must abide by the same requirements as visitors. In addition they must ensure that

<p>Equipment Ensure equipment and machinery is in a safe and serviceable condition • Equipment found to be unserviceable is isolated or removed from site to prevent further usage • Be accountable for tools and equipment required to perform the task.</p>	<p>Installation Ensure equipment being installed meets current safety standards, is installed correctly, is suitable for the purpose and is fitted by trained or qualified persons only.</p> <p>Safety Signage Provide accurate and adequate safety signage and cordoning equipment.</p>
--	--

Typical hazards A hazard in the context of Health and Safety is “A potential source of harm which could have adverse effects on a person or persons”. A risk is the ‘Likelihood that a person may be harmed or suffer adverse health effects if exposed to a hazard’.

The common hazards are slips, trips or falls. Slips are usually caused by poor maintenance or staff carelessness. Other causes include spillages, leaks, weather (snow, ice, rain), highly polished floors, moss

or leaf fall. Trips are also often the result of poor maintenance. Other causes include rubbish left in walkways, steps not being clearly marked, poorly fitted and worn carpet or floor coverings, trailing cables. Falls are most often caused by misuse or incorrect use of equipment or fixtures. Other reasons include over reaching from ladders, insecure ladders and platforms, climbing on shelving or chairs.

Poor lighting

Whilst slips, trips and falls are the most common causes of accidents, **lighting** plays a significant role in both health and safety within the workplace. With regard to safety, effective lighting makes it quicker and easier to see, and thus avoid, hazards. Slips trips and falls are far more likely in areas where lighting is poor or ineffective. The lighting should be appropriate to the environment and risk. Where lighting is not working, it should always be reported.

Another safety aspect of lighting relates to emergency lighting. Emergency lighting is used to guide people to exits during evacuations. Again, this should be checked and faults reported.

The final aspect of lighting relates to health. Poor lighting can cause eyestrain, fatigue, headaches, blurred vision, neck ache, double vision, lethargy, lower levels of concentration and more.

Other risks and hazards

Other common risks and hazards that security staff might come in to contact with:

- Conflict, violence, aggression and abuse
- Stress
- Criminal activity
- Anti-social behaviour
- Intoxicated people
- Excessive heat
- Overcrowding
- Malfunctioning or misused equipment
- Working at height
- Moving traffic or machinery
- Repetitive strain injury
- Fires and explosions
- Display screen equipment
- Hazardous substances
- Noise pollution
- Lone working
- Transmittable diseases
- Lifting and carrying
- Sharp objects

Other legislation

Noise at Work Regulations (1989) Amended 2006 defines three levels of noise at which employers are expected to take action.

First action level	80db(A)	Legal duty to provide hearing protection if requested by employees
Second action level	85db(A)	Take action to reduce noise as far as is reasonably practicable and provide ear protection in designated zones
Peak action level	140 Pascal (intermittent)	Protect staff and reduce noise

Minimising risk

The role of a security officer is to reduce risks and by effective patrolling, taking action or responsibility for removing hazards, and reporting hazards to supervisory staff.

All employers must assess the risks to their employees and other people who may be affected by their activities. Employers with 5 or more employees must also record the significant findings of that assessment. Risk assessments are used to identify the most important risks, identify measures to control the risk and comply with the law.

The assessment will identify the hazards present → evaluate the risks associated with those hazards → identify methods of prevention → record significant findings and review those findings.

If you identify a hazard during your duties that cannot be put right immediately → inform your supervisors or manager → make a note in the daily occurrence book and advise other members of the team about the risk, particularly at shift change or handover.

Awareness specific hazards

of Specialist risks/hazards include contact with: Oxidising chemicals in the hairdressing, industrial, manufacturing, pharmaceutical and cleaning sectors • Radioactive isotopes in the medical, research and waste management sectors • Noxious chemicals in the manufacturing, engineering and cleaning sectors • Potentially lethal engineering equipment and processes generally • Potential violence in the custodial sector • Exposure to noise.

Where operational profiles have identified a particular need specialist training should be provided.

Generic training Site specific emergency access and egress • Emergency points of contact and advice • Legal and procedural responsibilities.

Specialist training Specialist training on the hazards created by the process, procedure or activity, and how to deal with the hazards • Technical briefing on the security officer's responsibilities in regard to monitoring the process • Technical briefing on the objectives of the security officer's role or function in that specialist case • Where required, operations using a 'safety-man' or 'banksman'.

Security staff should: Be aware of potential hazards • Understand the risk assessment process and risks • Follow Health and Safety along with organisational policies and procedures • Use appropriate personal Protective Equipment, Personal Alarms, Phones and Radios • Be aware of procedures for loan working.

Security staff should know the hazardous substances stored or used within the site. This is imperative in order that risk can be minimised to staff and customers and that in the case of an emergency such as fire, or injury because of exposure to the materials in question, the security officer can be of maximum assistance to the emergency services. Companies must abide by Control of Substances Hazardous to Health Regulations (2002) (COSHH).

Security staff working within a noisy environment, such as areas clubs, areas where vehicles are loading or unloading or in areas with noisy machinery, can be exposed to noise above the second action level but this exposure is generally not daily. However, it is good practice to limit your exposure with security teams organising their activities so that security staff mix time spent in areas that are the subject of noise, and time in quieter areas of the site. Companies must abide by the Noise at Work Regulations (1989), as amended 2006.

Precautions against infectious diseases

Infection can be passed on by contact with bodily fluids. Risks to security staff are higher when searching (people, areas and lockers), when making an arrest, dealing with aggression and when administering first aid. There are steps that you can follow to prevent cross infection.

As a member of the security team you should always follow these guidelines: When searching, be aware of unguarded needles • Wear protective gloves and change them regularly as they may split with wear • Use the self search technique as discussed in the module on searching, getting staff and customers to empty their own pockets • Do not put your hands into areas you cannot see i.e. behind toilet cisterns, into bags or clothing • When patrolling industrial areas apply barrier cream as appropriate and according to the manufacturer's instructions • Where available, sharps boxes should be used to dispose of sharp objects, when not available sharps should be safely stored until a preferred method of disposal is available • When dealing with accidents or illnesses, protect yourself from contact with vomit, blood, excrement, etc, by using the first aid protection provided. If possible avoid contact with the victim • When cleaning up after accidents or injuries, use the recommended concentration of detergent to water • Ensure cuts, grazes or skin breakages are covered with a sterile dressing • After carrying out such tasks, wash your hands with copious amounts of hot soapy water • Contaminated clothing should be washed in hot soapy detergent to ensure any bacteria is destroyed.

Personal alarms and mobile phones

Security officers may be issued with communications equipment including radios, mobile telephones and other two-way alarm devices, but it is also common for most individuals to carry their own mobile communication devices. Make sure that these do not distract from critical operations and be aware of the risks of triggering a fire in some environments, or triggering a device during a situation involving terrorists. The use of such equipment in potentially hazardous circumstances needs to be comprehensively assessed and you must remain aware of your surrounding environment.

Safe routines

The best way to manage any risk is by prevention rather than cure. Part of that can be the establishment of safety conscious routines and 'safety culture'. Basic routines might include: Communication with all security staff should keep control advised of movements and activities • Avoid unnecessary risks • Security staff should always call for back up or report on situations if risk is apparent and avoid risk if possible • Dynamic risk assessment should be a key behaviour of all security staff • Reporting security and safety hazards and risks immediately and taking ownership of problems • Using Personal Protective Equipment.

Personal Protective Equipment

Person Protective Equipment (PPE) comes in many forms and styles and is provided to you to protect against hazards within the workplace. If you are issued PPE you **must** use or wear it. If you have an accident at work and the injuries were because you did not wear or use PPE, then you are unlikely to qualify for injury benefits or compensation. PPE includes High visibility (hi-vis) jackets or vests • Gloves (thermal and protective) • Tongs and sharps boxes • Thermal underwear • Hat or head wear • Boots or shoes • Ear defenders • Radios and earpieces • Safety goggles • PPE as required by the site.

Lone working

Security staff often find themselves working alone within a control room, gatehouse or when they are undertaking patrols, especially at night and at weekends.

Employers should: Check for medical conditions that would make lone working dangerous • consider whether the task is too risky for lone working • provide some level of supervision, such as regular contact calls • develop emergency contact procedures • provisions for lone workers in risk of violence • check specific/legal insurance requirements relating to the role.

Employees should: Make regular communications via phone, radio or visits • follow procedures which provide an automatic warning if worker fails to check in on time • use emergency alarms • work to an agreed itinerary • always be aware of their surroundings and continually engage in dynamic risk assessment • not enter an area or situation if the lone worker feels at risk • back off if they feel threatened • report concerns and incidents in the appropriate manner.




Manual handling




Manual handling operations regulations were introduced to reduce the number of injuries occurring as a result of lifting loads incorrectly. They cover the lifting, pushing, pulling, moving, carrying and putting down of a load by manual operation including persons. Before lifting any object, staff should consider the load, task environment and their capability. Whether the object needs to be moved, its weight and centre of gravity, whether it is safe to move, how easy it will be to grip, whether the surface creates other risks (cuts, splinters, etc), whether help is required to conduct the lift, the state of the outer package. Is the base stable for lifting?

Whilst conducting the lift: Place feet apart to obtain a balanced stance • The knees should be bent and the back should remain in the straight position • Before committing to the lift test the load, take a firm grip • Use the legs to perform the lift and keep the object close to the trunk of the body • Place the object down whilst again keeping the back straight and bend the knees as the object is lowered • **Avoid twisting action** • Ensure smooth movements wherever possible • Pushing should be preferred to pulling.

Safety signs

In order to protect staff and visitors within the site, instructions must be clearly displayed around the site to warn of danger, advise on personal protective equipment (PPE), identify safe exit routes and locations of first aid equipment, instruct staff on certain restrictions that are imposed throughout the site and to advise on use of fire fighting equipment. Signage conforms to common standards.

Label	Type of Sign	Colour	What it does	Examples
	Mandatory	White and blue	Must do as it instructs	Eye protection must be worn Fire doors must be kept shut
	Prohibition	Red, black and white	Indicates things you must not do	No smoking No entry
	Warning	Yellow and black	Warns of danger or harm	High voltage Slippery surface

	Safe Conditions	Green and white	Indicates fire exit doors and routes and identifies the location of first aid equipment	Fire exit First aid box
	Fire equipment	Red and white	Indicates type and use of individual piece of fire fighting equipment	Fire alarm Fire extinguisher
	Hazardous chemical	Orange, black and white	Indicates chemicals are being transported. The signs detail the manufacturer, type of hazard, emergency service advisory code, UN identification number and haulage company contact number	

Reporting procedures

Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (2013) (RIDDOR) regulations state that if there is an accident connected with work and an employee or a self-employed person working on the premises is killed or suffers a specific injury (including physical violence) or if a member of the public is killed or taken to hospital, that accident must be reported to the Health and Safety Executive (HSE) or the Environmental Health Department of the Local Authority.

The list of 'specified injuries' in RIDDOR 2013 (regulation 4) includes: • a fracture, other than to fingers, thumbs and toes • amputation of an arm, hand, finger, thumb, leg, foot or toe • permanent loss of sight or reduction of sight • crush injuries leading to internal organ damage • serious burns (covering more than 10% of the body, or damaging the eyes, respiratory system or other vital organs • scalplings (separation of skin from the head) which require hospital treatment • unconsciousness caused by head injury or asphyxia • any other injury arising from working in an enclosed space, which leads to hypothermia, heat-induced illness or requires resuscitation or admittance to hospital for more than 24 hours.

More details can be found in the following leaflet <http://www.hse.gov.uk/pubns/indg453.pdf>.

If any accident connected with work results in a person being incapacitated for more than seven days, it becomes a reportable accident. This includes loss of consciousness. It should also be noted that RIDDOR also requires that near misses, dangerous occurrences and exposure to dangerous substances are also reportable.

It is the responsibility of the employer to report all such occurrences. If a security officer witnesses an incident or accident, or is involved in any way, a written report must be submitted. It is the responsibility of the security officer to ensure that all necessary legal reporting is complied with, should a personal injury occur.

Reporting of accidents and ill health at work is a legal requirement. The accident may need to be investigated to determine the cause and recommendations made to ensure that the occurrence is not repeated. The following procedures should be followed in the event of any accident or injury in the workplace, including near misses.

- Make entries in your pocket book
- Complete the daily occurrence book entering details of the incident
- Complete an incident or accident report
- Complete an entry into the accident book
- Contact control or site management giving full details of the incident
- Contact the site health and safety officer giving full details of the incident

Accident books

Organisations must also ensure that all injuries, irrespective of how minor they might appear, are properly recorded in an accident book in premises covered by the Factories Act or where ten or more people are employed at any one time. Any employee who suffers a personal injury whilst at work must inform his or her employer as soon as possible after the accident has occurred, and it is the employer's duty to investigate the

circumstances of the accident.

The following information must be recorded in the accident book: The full name, address and occupation of the injured person • The date and time of the accident • The place where the accident happened • The cause and nature of the injury. Where the employer investigates an accident and finds discrepancies between what happened, and the employees reporting of the incident a record should be made in the appropriate part of the accident book • The name, address and occupation of the person making the notification if they are not the injured person.

Reporting general in The following procedures should be followed in the event of any accident or injury in the workplace, including near misses: Make entries in your pocket book • Complete the daily occurrence book entering details of the incident • Complete an incident or accident report • Complete an entry into the accident book • Contact control or site management giving full details of the incident • Contact the site health and safety officer giving full details of the incident • Ensure that you follow company procedures.

Dealing with a 1st aid situation If you are faced with a situation requiring first aid: Firstly check that you and the casualty are not in danger • When it is safe to do so, call for a first aider and or dial 999 or 112 for an ambulance if necessary • Your assignment instruction of site notices should advise you who the appointed person, or designated first aider is on the site. Ensure that you know who this or these people are and how they can be located • Make sure that you know the location of first aid facilities • Always work within the limits of your own ability, whether you are a qualified 1st Aider or not.

When to call emergency services When to call an ambulance can be a matter of judgement in general you should always call 999 if someone is seriously ill or injured, and their life is at risk. Examples of medical emergencies include (but are not limited to): chest pain • difficulty in breathing • unconsciousness • severe loss of blood • severe burns or scalds • choking • fitting or concussion • drowning • severe allergic reaction • eye injuries.

4. Principles of fire safety

Fire Triangle Three elements must be present for a fire to exist. If any of these elements is missing, a fire cannot occur.

Fuel , which could be paper, pallets, curtains, plastics, paints, petroleum, hydrogen, etc.	Oxygen , which could come from cylinders or the atmosphere.	Heat , which could be provided by sparks, friction, the sun, chemical reactions, electrical heat elements, etc.
--	--	--

Prevention of fire In general, fires can occur because of one of three reasons: Deliberately • As a result of breakdown or failure • As a result of accident or carelessness. Typical causes of fire include Poor storage of hazardous materials • Poor storage of combustible materials (paper in stairwells, waste bins that are not emptied, greasy overalls, etc) • Inappropriate use of portable heaters • Electrical equipment overheating or arcing • Machinery overloaded • Kitchen equipment and oils left unattended.

Legislation The Fire Safety Order 2005 in England and Wales, the Fire (Scotland) Act 2005 and the Fire precautions (workplace) regulations (Northern Ireland) 2001 places a legal requirement on all employers to undertake a fire risk assessment. The risk assessment is designed to: Identify fire hazards • Identify the people at risk • Evaluate the risk • Remove, reduce or protect against potential risk • Record and review assessments.
Every employee has a responsibility to take care and co-operate with the employer in complying with the legislation, and inform employers of any danger that is encountered. Security staff have a significant role to play due to their responsibilities.

Role security of It is a role of the security team to Identify risk and then to remove that risk wherever possible • Reduce the risk if it cannot be removed • Report the risk or the actions taken.
In addition to preventing fires, security staff have a responsibility for fire safety. This involves ensuring that: Escape routes are kept clear • Doors on escape routes are not obstructed and are secured correctly (not locked) • Fire doors are operating correctly • Signage and lighting for escape routes are operational • Equipment for tackling fires is secured correctly and operational • Faults on alarm panels and systems are reported immediately.






Classifications There are 5 classifications of fire. Class A (textiles, wood, paper, cloth) • Class B (liquids) • Class C (gasses) • Class D (metals) • Class F (cooking oils and fats). Electrical fires are not included as an official classification, as they can fall into any of the classifications. The reason being that electrical equipment is often the cause of a fire, rather than an actual fire type. **Class C and D fires should not be tackled by anyone other than a trained fire fighter.**

Fire classifications determine the actions that should be taken and fire fighting equipment that might be used. They also give an indication of the level of risk associated with a particular type of fire. Caution should always be exercised when dealing with fires. Even a small bin fire can hold hidden risks such as aerosol cans which can be extremely hazardous. Do not put yourself in danger.

Extinguishers There are five common types of material that are used in fire extinguishers to extinguish or suppress fires. The type of extinguisher that is used depends upon the fire. The five materials are: Water • Dry powder • Carbon dioxide • Foam • Wet or dry chemicals.

The body of all fire extinguishers is red and the labelling is colour coded to inform the user of the type of extinguisher. The labelling also provides instructions for the use of the extinguisher, and the types of fire on which it should be used.

Always use the correct extinguisher for the type of fire that is being tackled.

	Type	Label colour	Use on	Use
	Water	Red	Class A	<ul style="list-style-type: none"> Cools fire (removing heat) Aim at the base of the fire Never use on electrical fires
	Powder	Blue	Class A, B, Electrical fires	<ul style="list-style-type: none"> Smothers the fire (removing oxygen) Aim the jet directly at the base of the fire and coat all materials with the powder Care should be taken when using this extinguisher and avoid inhaling powder
	Foam	Cream	Class A, B	<ul style="list-style-type: none"> Smothers fires Aim at the jet at the rear of the fire and slowly work forward coating all materials Foam is water based so must not be used on electrical fires
	Carbon dioxide (CO ₂)	Black	Class B and electrical	<ul style="list-style-type: none"> Cools and smothers fires Aim at the fire Cone and nozzle of the extinguisher will be very cold
	Wet Chemical	Canary Yellow	Class F	<ul style="list-style-type: none"> Cools and smothers fires Aim towards the rear of the fire and work to the front.

Other types of Portable fire fighting equipment includes sand buckets and fire blankets. Sand can be used to smother small fires, usually class B and fire blankets are usually used to smother class F.

Fixed appliances include hose reels used for tackling larger class A fires.

Installed systems include: Sprinkler systems • CO₂ drenching systems • Foam flooding systems • Wet risers and dry risers. Sprinkler systems are located in the ceilings of buildings where an abundance of combustible materials are stored such as retail outlets and warehouses. Security staff should, as a matter of course, identify as early as possible where the sprinkler system emergency shut off valves are as if it is established that no fire exists, prompt action by the security officer may prevent many thousands of pounds worth of damage.

Wet or dry riser systems can be simply described as a network of vertical pipes located within multi-story buildings. Within the network are strategically placed outlet points to which the fire service can attach hoses. The system is designed to supply water to all levels of a building whilst reducing the need for additional hoses. The difference between a wet and a dry riser is that a wet riser system is constantly charged with water whilst the dry riser system remains drained and is charged with water by the fire service as required.

CO₂ or gas extinguishing agent drenching systems are designed to provide a high quantity of extinguishments in confined spaces. They are normally provided in areas that contain large electrical

installations, computers or PA equipment. When activated, the gases replace the air in the area so starving the fire of oxygen. These areas are well signed and the system will be supported by an alarm that sounds prior to discharge. On hearing the alarm, all persons located within the vicinity of such systems should vacate the area immediately (the time from alarm to release can be as little as two minutes). Anyone remaining within the area will be at risk from suffocation or hypoxia. Return to the area should only be attempted after authorisation from the fire service.

Foam flooding systems are installed in areas that contain flammable liquids such as fuel storage areas and inflammable storage areas such as alcohol stores. The system is designed to inject large amounts of foam into the area so eliminating the need for entry. The system is activated by a valve that supplies water, which in turn mixes with the foam-producing chemical, which is then pumped into the area containing the fire. It is essential that the activation valve is kept clear of obstacles that may inhibit access.

Fire doors are an effective method of preventing the spread of fire or simply to delay the spread of fire and smoke to aid evacuation.

Operating firefighting equipment

When using any fire fighting equipment always follow these simple rules: • On finding a fire, always operate the alarm first to warn others • Never put yourself at risk, only deal with situations you are confident in dealing with • Read the labels and instructions on fire equipment • Know the location of fire equipment and the sounds of the different alarms • Seek help. Never tackle a problem on your own • If in doubt GET OUT.

All details covering fire equipment and procedures are contained within your assignment instructions. Read them, they could save your life.

Fire control panels

The fire alarm control panel provides: Details on the location of the incident in a zoned system • Information on the extent of the area in which the incident is occurring • Early warning of incidents • Operators with information to provide intelligence to the emergency services • Security staff with the opportunity to take necessary precautions in responding to an incident.

Control panels are normally located in the control room.

Alarm indication

- A red indicator for each zone which must light up if there is an alarm in the zone
- An audible indication of the alarm

N.B. Red lights will only ever mean a fire alarm and must be responded to accordingly.

Fault indication

- A yellow indicator for each zone on the system
- An audible indication that must be different from the alarm

When the yellow light shows it means that something has happened that is different from what is normal and must be reported.

Mute switches

- Separate switches to silence the alarm and fault sounders

These are set up so that if switched off and another fault or alarm occurs the alarm will re-sound. NEVER assume that it is the same alarm or fault.

Reset switches

The reset switch is the only way to reset alarm conditions. If the condition has not cleared when the switch is used, the alarm will sound again.

Disable or inhibit function

There may be the facility to disable part of the system, e.g. during maintenance.

- There will be an audible and visible indication (different from the alarm and fault warnings)
- Cannot be muted and will remain until disablement removed

Reporting fires

The control panel provides valuable information that can be provided to the emergency services in the event of a fire. It can provide information on the location and spread of the fire and when combined with site knowledge, security staff can identify and communicate specific risks such as hazardous materials.

Response to Fire

On discovering a fire there are steps that should be taken to evacuate the building and to deal with the fire. The Home Office uses the acronym FIRE.

Find	Your may see or smell smoke, feel heat or witness items scorching, taste particles in the air, hear it or see staff panic and run from the scene. When patrolling you may suspect the presence of fire and there are procedures to follow to ensure your own personal safety as follows: Feel the door with the back of your hand • Try to view the area through a window • Look for signs of smoke escape around doors • Listen closely • You may be able to smell smoke • Listen for alarms • Check fire alarm panels for zone activation. NEVER OPEN THE DOOR as you will provide the fire with the necessary oxygen or reintroduce oxygen into the area of the fire.
Inform	The first thing you must do is raise the alarm. There are several ways in which you can do this: Use your voice. Shout FIRE as loud as you possibly can - Break the glass in an MCP (Manual Call Point) • Ring the fire warning bell (found on older sites) • Use your radio to contact control or site management • Use a land line or mobile phone to contact the control room, site management or the fire service. Raising the alarm as soon as possible will attract help and also warn others of the dangers. Early warning saves lives.
Restrict	On discovering a fire, and once you have raised the alarm to notify others, there are steps you can take to prevent the fire or smoke from spreading, if it is safe to do so: Close all windows and doors within the vicinity of the fire to reduce the air supply to the fire - Close all windows and doors on exiting the building • Remove combustible materials from the area of the fire • Isolate other areas.
Evacuate / Extinguish	When responding to a fire you can do either one of two things 1) Try to extinguish the fire if it is safe to do so. Before doing so, check to make sure that you have the correct extinguisher and that its size is sufficient to deal with the fire or 2) Evacuate the building and go immediately to the fire assembly point. Never try to use a second extinguisher. If the fire was too big to be put out with one extinguisher, it is too big for you to fight. Fire spreads very quickly and even a small contained fire can quickly spread, producing smoke and fumes which can kill in seconds. If you are in any doubt do not tackle the fire, no matter how small. You can put yourself at risk by fighting the fire. If in doubt get out, get out.

It is important that members of the security team remain calm at all times when dealing with a fire. If you are in uniform, your uniform will attract attention and you may be called upon to assist others in evacuating the building. If you remain calm others will follow your example making the evacuation of the building and the resolving of the problem easier.

Evacuation

Security staff play an important role when a building or site is evacuated. Members of the security team will usually have specific functions to undertake during the evacuation process, but even when this is not the case, their uniform leads to others seeking advice and guidance. The purpose of an evacuation is to get people out of the building or away from the site safely, efficiently and in an orderly fashion. It is a legal requirement for organisations to implement effective arrangements for access and emergency evacuation of employees and visitors. **Evacuation plans:**

- Provide details of different type of alarms, and messaging systems used in the event of an evacuation
- Identify safe escape routes
- Identify safe muster points
- Define the approach to evacuation
- Identify any procedures relating to roll calls
- Identify and define the roles of those involved in the evacuation process and in particular fire marshals
- Describe any responsibilities relating to maintaining or managing access points for the emergency services
- Describe shut down procedures for safety critical and security critical activities

In most premises, evacuation will be simultaneous, with everyone reacting to the fire alarm at the same time. Some larger and more complex premises might employ vertically phased evacuation where arrangements are designed to allow people who are not at immediate risk from a fire to delay starting their evacuation.

In addition to the general evacuation plan, any special arrangements for disabled people such as those with issues relating to mobility, sight, hearing or learning difficulties should also be considered. This is often considered within a **Personal Emergency Evacuation Plan (PEEP)**, which is specific to the individual and identify: Any specific needs of the individual • Staff responsibilities • Staff training requirements • Specific evacuation routes where appropriate • Refuge areas and specific evacuation procedures, such as the use of evacuation chairs.

Make sure that you understand the evacuation procedure. It will save time in an emergency, reduce the risk to the safety of those on site and allow you to be of more help to the emergency services. Failure to do so places those in the building at greater risk of injury and perhaps even death. Make sure that you:

- Understand your role in the evacuation procedure
- Know where the fire exits and escape routes are in the building
- The safest escape route might not be the one that is closest to you
- Are familiar with the locking systems on building exit doors used for evacuation. Whilst some exits will be through doors that are used in day to day operation, other exits will be through doors which deny access to the building but will allow escape in the case of emergency evacuation
- Be familiar with assembly (muster points)
- Be aware of and respond to people with specific needs during the evacuation process. The disabled old and young in particular could require additional help and support during evacuation. Others may be fearful or panicking and need additional assistance. However, in responding to individual needs you must not neglect your responsibilities to the other staff and this might mean co-opting support from a calm and able member of staff to assist in getting the person concerned to the muster point.

Do not wedge open fire doors as this can cause smoke to circulate more quickly and perhaps cut escape routes • Shut windows to reduce the supply of oxygen to the fire, where it safe to do so • Do not use or allow the use of lifts, unless they are part of a PEEP • Assist the emergency services where appropriate by keeping emergency access routes clear and providing site advice when requested • Do not re-enter or allow re-entry to the building until it has been declared safe by the police, fire service or authorised person • Remain calm at all times. If security staff convey a sense of panic, it is more likely that others will panic and evacuation will be less likely to be conducted in a safe and orderly manner • Discharge the duties that are required of you in the plan effectively.

Role of fire marshal A Fire Warden's daily duties may include checking that: • Exit doors are available for use, unlocked and unobstructed • Escape routes are clear of storage and combustible materials • Fire extinguishers are in position with seals in place • Fire safety signs are in position • Fire alarm call points are unobstructed • Fire-resisting doors are closed and functioning properly • Any malfunction of the weekly fire alarm test is reported • Any person with a disability who may need help to evacuate is facilitated • Any faults on the emergency lighting are reported.

Tasks in an emergency: Supervising or assisting the evacuation • Taking responsibility for Personal Evacuation and Emergency Plans • Checking that the evacuation has been completed and that everybody is off site • Undertaking the roll call.

5. Emergencies and the importance of emergency procedures

Definition **Emergency:** A situation that is unexpected, threatens safety or causes serious disruption and requires immediate action.

General security emergencies Flood • Gas Leak • Explosion and fire • Power failure • Accident and injury • Serious illness • Theft and criminal damage • Other crime including sexual and discrimination offences • Public disorder • Bomb threat or suspicious object • Failure of computer systems or equipment • Loss of keys • Weather or natural disasters • Hostage or duress situations • Major damage to corporate reputation • Extortion • General compliance breaches, etc.

Types

Door supervision Customer on customer violence • customer on staff violence • compliance breaches (particularly sale of age restricted items, licensing regulations and weights and measures) • substance abuse and overdose.

Static guarding sites Accidental contamination of public sewers, waterways or the atmosphere • chemical spill • product contamination • theft or compromise of secret processes.

Retail sites Customer on customer violence • customer on staff violence • compliance breaches (particularly sale of age restricted items, licensing regulations and weights and measures) • missing persons.

CCTV operations Compliance breaches (Data Protection Act and Criminal Procedures and Investigations Act) • system breakdown or failure of back-up procedures • passing information to unauthorised persons • unauthorised release of assets such as keys.

It is important that staff are aware of policies and procedures relating to possible emergencies, and have a good understanding of the environment in which they work.

Response to emergencies Site Assignment Instructions will detail the procedures for dealing with most emergencies and incidents. They will usually include

- Reporting chains and channels of command
- Limits of authority
- A number of planned 'set-piece' scenarios
- Emergency contact numbers
- Risk and threat assessments
- General and specialist instructions
- Floor and site plans
- Locations of key assets, resources, utility cut off points and vulnerable or hazardous equipment and substances
- Locations of and inventories for boxes and cupboards containing emergency equipment and supplies

Procedures

Where possible, follow Site Assignment Instructions. → When the situation is not covered by assignment instructions / events overtake planned responses *Be flexible, take responsibility and apply common sense and experience.*

Identify immediate hazards and the risks they present • Identify the assets and resources needed to safely tackle the emergency and find out if they are available • Prioritise between the different situations and the resources available • Continuously review the hazards and risks and evaluate the options • Act safely • **Decide, communicate, act and review.**

Your Behaviour Act quickly, be authoritative, remain calm, encourage others to remain calm and prioritise incidents and actions.

WHY?

Your uniform will attract attention
 If you panic, others will follow suit
 Your thoughts will be clearer
 The risk of injury to you and others is reduced
 You will communicate clearer and be better understood

HOW?

Do not rush around unnecessarily
 Keep people informed
 Offer guidance and support
 Reassure people
 Do not shout or raise your voice
 Remain professional at all times
 Seek assistance if needed
 Be courteous and respectful

**Dealing
others**

with Encourage others to remain calm:

- Ask people to
 - walk not run
 - not to raise their voices, or speak too quickly
 - to be patient when waiting by exit doors
- Keep people informed of the situation
- Seek assistance if the situation becomes unmanageable
- Show empathy when dealing with friends and family of unaccounted or missing people, but never allow them to return to assist in the search
- Seek medical assistance for those suffering from shock
- Try to keep the most disturbed segregated from the calm
- Evacuate those in distress first

**Making
emergency
calls**

1. Dial 999 or 112 (remember the prefix number to connect to an outside line)
 2. Give name and assignment address to operator
 3. Ask for required service (police, ambulance, fire brigade, etc.)
 4. Answer the questions asked by the emergency service. You are likely to be asked about the nature of the incident, the precise location, your contact details and name, information about site access etc. Provide any information requested as clearly and accurately as possible, if you cannot answer a question, say so.
 5. Ensure handset is replaced correctly
 6. If using a mobile, refer to the network user guide
- It is important that you remain calm and communicate clearly.

Personal Injury

Initial response: Assess the situation • Do not put yourself in danger • Make the area safe. Control the area by using bystanders if necessary • Remain calm as this will give the casualty and others confidence in your ability • Assess all casualties and attend to those that are unconscious first • Reassure those involved.

If you are not a first aider, shout or radio for help immediately. Either contact or get somebody to contact a designated first Aider.

**Unconscious
casualties**

1. **Shout for help.**
2. **Ensure that the airway is open.**
 - Check the mouth for obstructions and remove them.
 - Open the airway by placing one hand on the casualty's forehead and gently tilting the head back whilst lifting the chin using two fingers only. This will reduce the risk of them swallowing their tongue.
3. **Check breathing.**
 - Listen and feel for normal breathing for no more than 10 seconds.
 - Look for chest movements.
 - Listen at the casualty's mouth for breath sounds.
 - Feel for expressed air on your cheek.

**Recovery
breathing**

and If the casualty is breathing normally: • Place them in the recovery position if they have no obvious head or neck injuries • Get help from a qualified first aider • Check for continued breathing.

Chest compressions

If the casualty is **not** breathing normally and a first aider is not on the scene, you can start **chest compressions**: • Lean over the casualty and with your arms straight, press down on the centre of the breastbone 4-5 cm, then release the pressure • Repeat at a rate of about 100 times per minute • After 30 compressions, open the airway again • Pinch the casualties nose closed and allow the mouth to open • Take a normal breath and place your mouth around the casualties mouth, making a good seal • Blow steadily into the mouth while watching for the chest rising • Remove your mouth from the casualty and watch for the chest falling • Give a second breath and then start compressions again without delay.

Continue with chest compressions and rescue breaths in a ratio of 30:2 until qualified help takes over or the casualty starts breathing normally.

Responding to Severe bleeding**serious injuries**

- Apply direct pressure to the wound
- Raise and support the injured part (unless broken)
- Apply a dressing and bandage so that it is firmly in place

Broken bones and spinal injuries

In such circumstances, casualties should only be moved if they are in immediate danger. Moving the casualty could make the situation worse, causing long-term injury or death. Always obtain expert help.

Burns

For serious burns, medical help should be sought. When dealing with burns:

- Cool using cold water until the pain is relieved. This could take 10 minutes or more but should not delay the casualty getting to hospital.
- If it is a chemical burn:
 - the affected area should be flooded with water for 20 minutes
 - contaminated clothing that is not stuck to the skin should be removed
 - continue to flood the area on the way to the hospital
 - do not contaminate yourself

Eye injuries

All eye injuries are potentially serious.

- If there is something in the eye, wash out the eye with still water or sterile fluid to remove the loose material.
- Do not attempt to remove anything that is embedded in the eye.
- If chemicals are involved;
 - Wash out the eye with still water or sterile fluid for at least ten minutes, whilst gently holding the eyelids open.
 - Ask the casualty to hold a pad over the injured eye and send them to hospital.

Summoning help

Give information on: • **Exact Location of incident** • **Telephone or contact details** • **Help required** • **Access to the scene** • **Number of casualties** • **Extent of injuries.**

Reporting

Recording and reporting an event is essential and should be kept in respect of all first aid incidents. However, detailed reporting *during* a serious incident is seldom possible. Use your personal security notebook during the event to record key words and facts coupled with timings which will help you later to write your report.

In reporting you should ensure that you cover the 'who why what where when & how'. Examples might include:

Who was injured - by whom - who reported it - who discovered it - who arrived or left - who made what order or made which decision?

When was it discovered - was it reported - were the emergency services called - were the management team notified - did various people arrive - were casualties taken off site - was the emergency declared to be 'over'?

Where was the emergency - were you when notified - were the most serious casualties - were the offenders - were the witnesses who made key reports?

What triggered the incident - happened - happened next - might have happened had you not made a certain decision?

Why did it happen - did you take certain decisions - were casualties taken to X instead of Y - did you arrest an

individual?

How did it happen - did you bring a certain situation under control? Stick strictly to fact, avoiding hearsay and rumour. However, a post-incident report may require professional opinion as to how the situation was caused and how it might have been handled more effectively.

Following a situation involving 1st Aid, the accident book must be completed.

Factors that make people vulnerable People under the influence of drugs and/or alcohol can be vulnerable because they can: • Have reduced inhibitions • Lack spatial awareness increasing the likelihood of hurting themselves or others • Display aggression • Become overly gregarious • Have changed perceptions of their abilities and limitations • Have decreased ability to make considered decisions.

Individuals who have been separated from their friends or appear lost, along with someone receiving unwanted attention over a period of time or being threatened or followed can be considered vulnerable. Victims of domestic violence can be at an increased risk of harm or assault, which can be fuelled by alcohol. Young people, particularly those under the age of 18 can be especially vulnerable in a lot of situations. Someone who has been targeted by a sexual predator can be more vulnerable. Recognising this type of behaviour is discussed next. Someone having a physical or learning difficulty. Someone having a physical or learning difficulty.

Behaviour of sexual predators A sexual predator will often target victims based on the following factors: Appearance, Race, Location, Gender, Availability and Vulnerability.

How to spot sexual predators and what actions you can take: • A sexual predator could be a lone male. If you see a lone male pestering a woman, you could approach the woman to access her safety, inform the venue management or call the police • Sexual predators can use drugs such as Rohypnol to facilitate their crimes. If you find suspect drugs that you feel may be used to facilitate a crime then call the police • If you witness a heavily intoxicated female exiting the venue with a male, consider approaching them to seek clarity on the relationship to ensure the safety of the female • If there is a regular lone attendee at your venue, you will often recognise who they are. Do they often leave with a different woman every time and do these women appear intoxicated? If so this may be an indication of a sexual predator.

Actions to take When a person is identified as being vulnerable and at risk of harm, it is important that security staff take responsibility. This might include • Seeking the help of street pastors or street marshals if a scheme is running in the area • Calling a relative to assist, particularly in the case of a younger person or vulnerable adult • Calling for a licensed taxi to take the person home • Using safe havens or other local initiatives run by the likes of St Johns Ambulance • Calling the police to assist the person.

Reporting child exploitation There are a number of warning signs that crimes associated with child sexual exploitation may be taking place. These include: • Children and young people in the company of older people or anti-social groups • Young people acting in an inappropriate and sexualised way with adults/older people • Children and young people showing signs of intoxication, particularly if they are with older men who are not intoxicated.

Visible signs that children are being trafficked could mean child sexual exploitation is taking place. Warning signs of this include: • Children and young people arriving and departing at a given location with different adults on the same day or over a period of time • Children and young people getting into and out of a number of different cars • Groups of young people using hotels or bed and breakfast establishments with older men.

Children who are being sexually exploited may show changes in behaviour or start to look different, this could include: • Unexplained changes in behaviour, such as chaotic, aggressive or sexual behaviour • Self-harming or suicide attempts • Showing fear in certain company • Having cuts and bruises from assaults • Having unaffordable new items such as clothing and mobile phones • Developing expensive new habits such as alcohol or drug use.

Security staff who suspect that child sexual exploitation is taking place should contact the Police. If they want to remain anonymous, then they can call Crimestoppers on 0800 555 111.

**Signature
behaviour**

We must consider then, the types of signature behaviour that may indicate that such activities are taking place, or being planned. These may include:

- Someone asking unusual questions about the site/venue, for example:
 - How many people it holds
 - What sort of people attend
 - Questions about procedures, e.g. “What would you do if this happened?”
 - Questions concerning security arrangements
- Someone loitering or walking around the outside of the venue and possibly taking photographs or sketching entrances and exits, car parks (car parks directly under the venue), pillars, columns, load-bearing struts, fire exits, assembly areas, loading bays, etc.
- Someone tampering with utilities.
- People making a brief visit to the premises and leaving immediately.
- The testing of security devices, systems staff and procedures to see how effective, resolute and knowledgeable they are, paying particular attention to CCTV camera locations and other security precautions.
- Testing security by breaching restricted areas.
- Isolated items such as bags or packages left anywhere in the venue or any object that appear to be out of place. Whilst these may not necessarily be terrorist devices, they may have been placed to see how long it took them to be detected and to see what happens once they are detected.
- Person with forged, altered or stolen identity documents, documents in different names.
- Multiple sightings of same suspicious person, vehicle, or activity
- Parked vehicles with people inside or empty parked vehicles left unattended for long period
- A person that is inappropriately dressed for the season or location

Behaviour that is ‘out of place’.

Actions to take in the event of a security threat Terrorist attacks are normally carefully planned and researched, and that planning and research may in its implementation, leave clues or indications that such an attack is being prepared. Security staff are often well placed for detecting such signs. The following behaviours or events **could** indicate terrorist activity:

Hostile reconnaissance, particularly the observation of patterns of behaviour, the drawing of sketches and photography of key and vulnerable locations such as car parks (particularly underground car parks, or car parks directly below the venue), pillars and load-bearing struts, fire exits, assembly areas, loading bays, and entrances.

Dry runs or practice runs, particularly the parking of the vehicle in a parking bay near or adjacent to the venue, or under the venue, and the driver walking off or decanting into another vehicle. Whilst, in a city centre, such activity may not necessarily be unusual, note should be made of the vehicle details and the individuals concerned, including and where appropriate, details of when they came back to pick up the vehicle - particularly if the people concerned to seem otherwise suspicious. Such details, particularly if repetitive, should be immediately passed to the police for checking and intelligence evaluation. If the situation is deemed to be urgent dial 999, otherwise call the counterterrorism hotline on 0800 789 321.

If the security staff are professional, alert, inquisitive and proactive, the likelihood of your premises being targeted reduces. Also, be aware that those who pose a terrorist threat are not always strangers, they can also be your work colleagues. If your colleagues are acting suspiciously, behaving in a strange manner or perhaps promoting fundamentalist beliefs of any sort, always raise your concerns.

Photographers Security staff have no right to prevent individuals from taking photographs: In a public place (whether or not the photographs concerned are of private property) • In a private location (unless it is expressly forbidden or requires a permit which has not been granted).

Security operatives cannot delete images, seize cameras or prevent members of the public from taking photographs in the above cases. The police have additional powers to prevent the use of photography for terrorist purposes, however, these cannot be used to prevent a member of the public / journalists capturing images of a public building.

When dealing with suspicious photographers, ensure that you question them politely, and if there is reason for concern, report the incident to the police immediately.

Monitoring incidents

Security staff must be able to apply their skills in respect to all of these risks. However, none of these behaviours on their own necessarily indicate that a person is either acting antisocially or as a terrorist. Security staff should:

- Avoid focusing on a single group or race
- Not jump to judgement unless the evidence is clear
- Observe and take details to confirm suspicions
- Report any suspicions they may have immediately
- Act quickly when suspicion is strong or confirmed
- Remain alert to the threat

Security staff should know the usual in order to identify the unusual. Terrorism and extremism crosses all boundaries there are such groups in all nationalities, from all religions and from all political persuasions.

Detecting, Detering and Preventing Terrorism

Ways the security staff can deter the likelihood of an attack, or reduce the effects of an attack should they occur include:

- Regular and high profile patrolling
- Regular, thorough (and highly visible) searches of the premises
- Always investigating unattended bags or packages
- Challenging suspicious behaviour
- Proactive and visible client screening and profiling, within the limits of current legislation
- The reporting and recording of all suspicious incidents, including to the terrorist hotline where appropriate
- Highly visible, enquiring, inquisitive and proactive presence
- Close and visible liaison with police and security agencies
- Ensuring entrances and exits are properly secured
- Follow procedures and be aware of the procedures associated with evacuation during a terrorist threat or incident
- Immediately reporting incidents to the police using the 999 service.

Awareness:

- Door supervisor should be knowledgeable about the location of their premises and neighbouring areas and buildings
- They should have knowledge of the premises procedures for suspected terrorist activities
- They should be aware of current threat assessments
- They should be aware of potential risks of terrorist activity

Evacuation procedures

When planning their response to a terrorist attack, many organisations have followed or developed a policy of 'assess, evacuate and disperse' rather than 'evacuate and assemble'. This means that employees and visitors **do not** go to the fire assembly area, but rather get clear of the area and telephone in to check when the situation receives the 'all-clear'. Following on from that, fire alarms **are not used** for the evacuation, since doing so would trigger an automatic response of going to the assembly area. Security staff should follow the evacuation plan and assignment instructions.

When evacuating and dispersing, encourage clients to go, and stay, well beyond the cordon line. A recent attempted bombing in London involved the planting of substantial secondary devices directly on the cordon line.

Evacuate and Assemble: Sound the fire alarm → Assemble at the fire assembly point

Assess, Evacuate and Disperse: Don't sound the fire alarm → Ask people to leave, stay away from the cordon line and phone in to check if they can return.

Remember, site assignment instructions take priority and follow them as far as is practicable.

Continuity plans

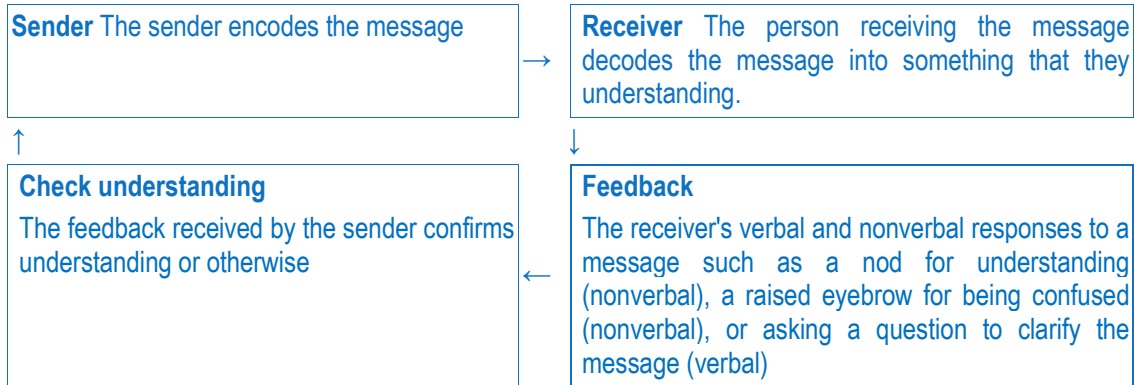
A growing number of businesses now undertake business continuity planning. This involves identifying those part of the business that an organisation cannot afford to lose in the event of an emergency or incident and how to maintain the operation of those aspects of the business should an emergency or incident arise. The purpose is to reduce or avoid disruption to the organisations, to reduce downtime and prevent business failure. A properly developed Business Continuity Plan, consideration will be given to the business needs in relation to its:

Consideration	Examples of considerations (not exhaustive)
People	<ul style="list-style-type: none"> • What would be the line of command if key staff were out of action • How would the business deal with people not being able to get there place of work • If the business was relocated, would the required level of trained staff be available.
Premises	<ul style="list-style-type: none"> • What would happen if a premises was lost – would there be an alternative?
Technology and assets	<ul style="list-style-type: none"> • What would happen if particular critical assets were lost or inoperable. • Does the business have access to duplicate assets or could it establish different processes
Information	<ul style="list-style-type: none"> • Is financial, customer and commercially data secure, backed up and duplicated. • Is the data accessible and how quickly could it be accessed
Supplies and Partners	<ul style="list-style-type: none"> • For businesses that are dependent on the secure and reliable supply of facilities, what would happen if the primary supply failed • If a partner was unable to provide a service, is there an alternative

The continuity plan is usually a high level document, written by senior managers or consultants employed by the customer. Where a plan exists, the role of the security staff is usually to: Play their part in testing the plans. The best plans are tested. • Perhaps providing an input on security specific issues and procedures • Following instructions in the case of an emergency.

6. Important communication skills and customer care

Communication Process Communication is the parting or exchanging of thoughts, opinions or information by speech, writing or signs & conveying information electronically or manually. Exchanging information without creating understanding does not create communication. There are many models for communication but essentially, it is a 4 stage process



Failure in any of these essential areas will result in information is not communicated effectively → The intended message is not understood = “a breakdown in communications”. Within the context of a security or safety role, this can be catastrophic.

Barriers to good communication	Physical & Environmental	→	Poor/faulty equipment, alarms and systems - distance apart - background noise, lighting - damage to signage
	Process failure	→	Incorrect documentation - Failure to send information to correct parties - Lack of clarity reporting lines – Misunderstanding of responsibilities
	Attitude	→	Complacency - Assumption - lack of concentration and interest - Pre-occupied
	Emotion	→	Stress - Anger – Anxiety – Nerves
	Linguistic(sender)	→	Message lacks clarity - Accent, jargon, slang - Poor choice of language - Poor choice of communication method - Body language
	Linguistic (receiver)	→	Unable to understand the subject - Hearing disabilities - Literacy skills - English as a second language

Non-verbal communication

- *Facial expressions:* The face is highly expressive and can convey emotions without us saying a word. The expressions tend to be common across cultures and in many ways, provides a universal language
- *Posture and body movements:* The way that people carry themselves conveys a lot of information about our interest and attitude.
- *Gesture:* We express ourselves with gestures and in particular hand movements to re-enforce or emphasise what we are saying.
- *Eye contact:* The way that you look at somebody can communicate many things including interest, affection, hostility and attraction. Eye contact is also important in maintaining the flow of conversation and gauging the other persons response
- *Touch:* We communicate through touch. This is less of an issue in the world of work but the nature of your handshake, approach to searching etc, conveys a message about you.

In addition, the way we dress and the distance we stand from each other also convey messages to the recipient.

Verbal communication

<p>Oral One to one communication, meetings, telephones, video conferencing, audio tapes/CD playing spoken message, radio, intercoms or public address systems.</p>	<p>Written Letter, memo, report, manuals, fax, e-mail, instant messaging, posters and signs, text message, daily occurrence book, registers, accident logs, notice boards.</p>	<p>Multimedia Internet, intranet, TV/Video, CD ROM.</p> <p>Other Pagers, alarm activation, signals.</p>
---	---	---

In terms of spoken communication, voice is important. It's not just what you say, but how you say it.

- The words we chose can convey intelligence or interest.
- Our timing and speed of delivery can convey interest and excitement
- Our tone and inflection and convey interest and emotion. Tone alone can convey sarcasm, anger, affection and confidence
- We can use sounds to convey interest and provide feedback

Active listening There are two parties to communication, a sender and a receiver. Most of us do the sending reasonably effectively but the listening can be a different matter. Instead of listening, people may be distracted, or thinking about what they are going to say next. Active listening is a structured way of listening and responding to others.

It focuses the attention on the speaker in order to understand what he or she is saying → The listener does not have to agree with what is being said, but this does indicate that the listener understands → The listener will not jump to conclusions and will not interrupt the speaker. Communication is then more considered.

The key features of active listening are:

- The listener is focused on the speaker, avoiding other distractions
- The listener seeks not to be judgmental about the speaker or their views, setting aside their own prejudices and opinions
- The listener focuses on both the spoken and the body language of the speaker, listening with their ears, eyes and other senses
- Avoid agreeing or disagreeing with the speaker, but allow them to develop their train of thought
- Be involved in the communication, responding to questions and use non-verbal techniques to signal interest in what the speaker has to say. Make notes and ask questions
- Where appropriate, repeat back to the customer to demonstrate attention and understanding.

Questioning

The use of questions is an important aspect of the communication process. Questioning can

- **Clarify an issue** → They are an important tool in developing understanding and a key aspect of the feedback process.
- **Build rapport** → They can be used to create a discussion, demonstrate understanding and perhaps encourage the sender to develop and extend their contribution.
- **Demonstrate understanding that the listener is indeed listening** → This is an important aspect of active listening.

The type of question that is asked is determined by the type of response that the questioner is seeking.

The primary types of question are

Open questions	Closed questions
<i>How could we improve safety on the shop floor?</i>	<i>Could safety be improved on the shop floor?</i>
<i>Can you describe the assailant?</i>	<i>What was the gender of the assailant?</i>
Possible range of answers are much wider	<i>Answers are limited to yes or no, male or female, or I don't know</i>
Encouraging the respondent to speak freely would possibly provide more information. Open questions are used for gathering new information, encouraging discussion, helping develop a train of thought and building rapport.	These questions encourage a short and restricted answer. This type of question is useful for probing for single facts or confirming understanding, but they are not useful when it comes to gaining new information.

When phrasing a question, consider the type of information that you are trying to obtain or why you are asking

the question. Think of the person that you are asking and how they might respond to your question.

Will you get an honest answer or the answer that the person thinks that you want to hear?

Will they be willing to respond or could they feel threatened or become defensive?

Good communication

The importance of good communication cannot be over emphasised. Good communication supports:

Organisational effectiveness:

- Reports are completed accurately, on time and sent to the right people. *This ensures that people are working on the correct information, that the information can be applied when it is required and ensures that those within the organisation that need to know, do know.*
- Completion of operational logs and register in accordance with company procedures. *This will ensure that the information is completed in accordance in a common and agreed format that also creates an audit trail which will improve security provision.*
- Timely completion of investigations.

Effective team working:

- Effective shift handover.
- Sharing information to ensure your colleagues can complete their tasks effectively and that they are able to support you in your role.

Effective service to customers:

Ensure that you deal with customers problems promptly and in a satisfactory manner.

Communication technique considerations

• Checking understanding through feedback • Providing an audit trail • Providing immediate communication • Conveying a message to a limited or wider audience • Communicating locally or over a distance • Providing greater consistency of message • Requiring action from receivers, others are passive.

There are several reasons why people fail to receive or understand information communicated to them and you should be fully aware of these. Firstly, you must consider:

Type - The type of information to be communicated, which relates to:

- The complexity of the information
- How quickly the information is required
- The intended target group for that information

How - Having considered what is to be communicated, the next decision is how to communicate it.

- The language that is used and how the communication is structured.
- Geographical and environmental considerations: If information is to be communicated over distances, or perhaps the sender and or receiver are in a noisy or busy environment, the method of communication would need to be considered.
- The level of confidentiality: For the most confidential information, secure communication paths must be selected.
- Whether feedback is required: Some techniques such as one-to-one meetings provide a natural opportunity for feedback. Other techniques such as video provide less of an opportunity for feedback.
- Is there a requirement for an audit path or a record of the communication? If so, written communication might be more effective.
- Is there a requirement to get a consistent message across to a range of people? If so written or media based techniques might be more appropriate.
- The urgency of the communication: In an emergency state the telephone, radio and other oral techniques might be more appropriate.

Circulation - Its circulation. The considerations might include:

- Who needs the information and why - will it promote effective team working.
- When they require the information.
- What will be the impact of sending or not sending the information?
- How would they expect to receive the information and what is important to the recipient.
- Feedback - does the understanding of the recipient need to be checked?

When communicating any information, irrespective of the method used, the sender should always ensure that the information is **Accurate, Brief and Concise**.

Customer Service

Customer service is one of the most important aspects of any business. Successful businesses tend to be proactive in defining and understanding what their customers really want, and putting systems in place to maximise client satisfaction. As the security industry is a service industry, providing high quality customer service is critical to the success of any company and security officers play an important role in the delivery of service to the customer.

Customers can be broadly categorised as **internal and external customers**. The significance of classifying customers in this way is that it can help identify their differing needs.

Internal customers are those people in your company that you provide your services to in order to deliver your company's products or services. They are your colleagues and co-workers.

External customers are said to be those people that actually buy your company's products or services. They are your pay cheque.

For security personnel, internal customers are those within the security company that they work for, whilst external customers are those to whom the contract service is being sold. If you are a security officer working for a contract security company, working in a shopping centre, the shopping centre is the external customer. However, security staff tend to have a more complex set of relationships. As well as working for the security company, they are often a part of the client's delivery team with significant contact with the customer's customer. In these cases the external customer could be seen as the customer's customer.

Another way to categorise customers is whether they are direct or indirect.

Direct customers are those that pay you for the service that you provide, and those that you work with in providing this service. The relationship is mutually supportive; there are rewards and expectations on both sides. The client wants a certain standard of service, for which they pay an agreed remuneration. The supplier, or the security officer, provides a certain level of expertise, for which he or she expects payment. Direct customers would include Your employer and your employer's customer.

Indirect customers are those that do not directly pay for the service that you provide, but those with whom you react during the course of your duties and who might be affected by your actions. These include Colleagues • Visitors • Sub-contractors • Emergency service personnel • Delivery/dispatch personnel • Neighbouring companies • Local residents • Telephone callers • Those using the services provided by the company • The customer's customer • Statutory agency staff.

The precise needs of internal and external customers or direct and indirect customers will be determined by the activities of the business. It is the role of security staff to understand the business, the expected outcomes and client mission statement, and both the employer's and the client's expectations on the way that customers are approached. Much of this will be covered in the Site Assignment Instructions, but will also usually be addressed in company and site inductions.

Customer expectations

Customer expectations will vary from site to site but are likely to include: • Provision of suitable and trained personnel that is knowledgeable and communicative • A quality service that is value for money • Contractual duties and responsibilities to be fulfilled and evidence of achievement through an effective audit trail which measures company performance against these set targets • Regular visits from those managing security • Problems solved quickly • The truth not excuses • Welcoming and courteous staff • Staff show common sense • Continuity of service. Achievement of key performance indicators and service level agreements.

Specific customer needs

Many organisations produce policies and procedures for dealing with customers with particular needs. The needs might relate to Physical impairment such as difficulties with mobility • Learning difficulties • Sensory impairment such as those with difficulties seeing or hearing • Those that have difficulties reading, writing or understanding English • Those under the influence of drugs or alcohol. It is important that you understand the policies in operation and the support that can be provided by the organisation in which your security team operates. Once again, much of this will be covered in the Site Assignment Instructions, but these issues will also usually be addressed in company and site inductions.

Principles of customer care

Good customer service is essential to the success of any business and as a member of the security team. You have a vital role to play in this area. Good customer service: Encourages customers to return • Builds confidence and earns the respect of the customer • Defuses potentially aggressive situations • Increases the level of trust

between you and the customer • Assists when dealing with emergencies • Maintains the reputation of the business • Maintains the reputation of the security industry • Increases the probability of stronger profits, the expansion of the business, and greater job security.

Security staff are often the first contact on the site, first impressions count. It is important that you understand how to promote good customer service. Therefore, it is important that you understand what promotes good customer service and how to prevent poor customer service. Client expectations will vary from site to site but are likely to include: The provision of suitable, trained, knowledgeable and communicative personnel • A quality service that is value for money • Key Performance Indicators and Service Level Agreements are delivered in accordance with the contract • Achievement of key performance indicators and service level agreements • Regular visits to the site from those managing security • Problems resolved quickly • The truth, not excuses • Staff that are welcoming and courteous towards visitors and staff on site • Staff apply a common sense approach to their role and can work unsupervised • Continuity of service.

Examples of **good customer service** include:

- | | |
|--|---|
| <ul style="list-style-type: none"> • Being clear and concise when communicating information • Establishing rapport • Carrying out your duties in a thorough, responsive and competent manner • Being observant and vigilant at all times • Treating people with respect • Being courteous and enthusiastic | <ul style="list-style-type: none"> • Taking pride in your appearance, your work, the company you work for and the environment in which you work • Offering help and assistance when required • Treating others the way you would be expected to be treated, with respect |
|--|---|

Examples of **poor customer service** might include:

- | | |
|---|--|
| <ul style="list-style-type: none"> • Poor understanding and knowledge of your job role, the tasks you are required to carry out, the site layout, and emergency and operational procedures • Failing to co-operate with company policies and procedures • Poor communication skills and using jargon | <ul style="list-style-type: none"> • Lack of commitment or poor attitude towards customers or work related tasks • Failure to acknowledge customers • Evasion or failure to deal with problems or issues • Discourtesy |
|---|--|

6 Golden rules There are 6 golden rules of customer service that, if followed, will increase the chances of the customer remaining loyal to your company or customer. The emphasis placed on each of the six rules will depend upon the situation that we are dealing with, or in which we are involved, and apply to all categories of customer.

1. Acknowledge the customer Security staff should Greet the customer, make them feel welcome and use eye contact • Make every effort to assist or help the customer • Avoid delay in acknowledging or responding to the customer. This should be a feature of your approach, irrespective of whether you are dealing with a problem or not.

2. Establish the customer's needs Security staff should Establish the needs of the customer. Gather all relevant details and facts • Prioritise the response to customers in order of need or urgency. Acknowledge customers who are considered to be of lower priority and inform them that you will be with them as soon as possible or find alternative ways of dealing with them • Identify the mood of the customer and think carefully about the approach you will take • Will they or have they had to wait for any considerable time? What can you do to make their wait less tedious or stressful, i.e. is there a comfortable seating area, are there magazines to read or can they obtain refreshments whilst they wait • Keep the customer informed at all times if delays occur and ask if they are able to wait? Again, this should be a feature of your approach, irrespective of whether you are dealing with a problem or not.

3. Put yourself in the customer's position (empathise) Security staff should Listen carefully to the customer and acknowledge by responding verbally or by using non-verbal communication • Work together with the customer and assist them wherever possible, i.e. with the completion of documentation, whilst searches are being carried out, or with location of stock or areas they wish to visit • Explain the rationale behind certain procedures if resistance is met at any time to establish full understanding • When people are annoyed,

inconvenienced or upset, their manner can change and they may become aggressive. However, by showing empathy, the customer will believe the member of the security team is on their side, or at least understands their position and may become calmer.

Empathy is defined as "...imaginatively entering into another person's feelings."

Before speaking to or assisting a customer, a security officer should consider how they would feel if they were the customer. Would what they say to the customer be acknowledged or accepted • Aggravate any given situation • Sound condescending to that particular individual. Again, this should be a feature of your approach, irrespective of whether you are dealing with a problem or not. In following this approach you may need to carefully consider age and culture. For example, some hand gestures may be considered friendly in one culture, but hostile or offensive in another.

4. Accept responsibility When we say 'accept responsibility' we are not suggesting that you declare "It's all my fault!" The responsibility that you are taking on is to find acceptable solutions or compromises or solutions that allow both parties to achieve an acceptable number of their objectives. The customer's objective may be to speak to someone in the technical department; yours may be to ensure that company policies and procedures are complied with. Security staff should ensure that any task taken on by them is seen through to a satisfactory conclusion • Keep the customer informed on their progress if relevant • Make sure the customer is satisfied with the outcome of their actions.

In order to provide a satisfactory conclusion to customer's requests, information will need to be supplied by the customer. This can be done simply by asking the customer questions to establish facts and gather details • Confirming that the details are correct by reading them back or talking through the facts with the customer • Clarifying areas of uncertainty with the customers • Identifying the customer's order of priorities regarding their requests and demands • Control the flow of the conversation by using assertiveness or by using open and closed questions. Again, this should be a feature of your approach, irrespective of whether you are dealing with a problem or not. Clearly, if you are not dealing with a problem or new area of activity, you would be likely to spend less time informing the customer of progress or checking that they are satisfied.

5. Involve the customer in the solution Security staff should be fully aware of the options available to them and their limitations • Flexible in their approach to finding a satisfactory solution. Compromise is a useful tool. Most of the time, all a customer will be seeking is advice. It may be as simple as asking for directions. You may not have the answer to the question but by asking others or advising the customer of an alternative source that may have the information that they require, you will be providing a satisfactory level of customer service and people will appreciate your help.

6. See it through You should always be seen to be offering the best level of service possible. As a member of the security team, you should provide to customers Alternatives • Support until the matter is resolved • Action to resolve the problem • Extra information.

We have mentioned earlier that you should only promise what you are capable of and authorised to provide. A good ground rule is to be very aware of what the limits of what you can do are, and, when issuing promises, always promise slightly less than you can deliver. In this way, you can always deliver slightly more than you promise, whereas if you make an offer but can only deliver slightly less, you will look inefficient and the customer may feel that you have broken your word. **Under promise, over deliver**

Answering the phone Be prompt and don't keep the caller waiting • If you are going to be away from your desk, put the phone on divert if you can or get a colleague to take messages • Answer the phone with a smile – it helps you come across in a more friendly way • Answer the phone in accordance with company guidelines. If they do not exist, make sure that you introduce yourself or your function properly eg "Good afternoon, reception security officer speaking" or "Good morning, Mike Turner, security team speaking" • Establish the needs of the caller quickly. Phrases like "How can I help" will assist • Use open questions to find out the facts and closed questions to clarify understanding • Answer questions promptly and clearly. If you do not know or can't help, tell the caller what you can do for them • Give conformity feedback on occasions to show that you are still engaged if it is a long call eg "I see", "Yes", "I understand" "Oh dear" etc.

Making a call • If appropriate try and make the call when it is convenient for the other person. Clearly, this is not always possible, particularly in a security role • Be clear about what you want to say and the purpose of the call •

Introduce yourself properly • Do not put off the difficult calls that you are nervous about making.

Tip: An approach that some people use if circumstances allow is to stand up when making a call to improve levels of confidence.

General phone etiquette Be polite and courteous at all times • Use clear and concise language • Give the caller or the person that you are calling your full attention • Keep focused and do not interrupt with pointless questions • Ensure urgent incidents are dealt with quickly and follow assignment instructions • Repeat names, and contact details back to the caller to ensure that you or they have got them right • Double check all vital information • Agree any actions that need to be taken • Make notes before or immediately after the call if you are going to require the information again • Complete any logs or records that are required • Ensure that messages received are accurate and pass them on in a timely manner • Recognise the limits of your own authority • Make sure that you manage your time on the phone • Maintain confidentiality.

Dealing with difficult callers Remain polite and do not get drawn into an argument • If the call relates to a complaint, let the caller vent their anger and summarise the key points of their concern to show that you have an understanding. Take responsibility • Speak clearly and take your time • Show empathy where appropriate for the callers feelings • Summarise to show understanding and engagement • Remain professional – what you think, what you say and how you say it are not always the same thing.

Radio practice best • Check that it is properly charged and working on receipt, or prior to undertaking a patrol
 • Use standard radio protocols to start and end transmissions. Call signs are often used to identify yourself at the start of a transmission.
 • Use clear and concise language, using the phonetic alphabet if spelling out such things as number plates
 • Ensure that you use the equipment correctly and do not block the communication of others by miss-operation of the equipment, communicating in an inconcise manner, or chatting.

In an emergency you should state 'urgent message' and the radio controller stops other traffic on the network and switches the radio to talk through mode. In an emergency, you should state the location and pertinent details of the incident.

Pro-Words

Pro Word	Meaning
Over	This is the end of my transmission and a response is required
Out	This is the end of my transmission to you and no response is required
Out to you	I am finished with the communication and am about to call another station. Do not reply
Received	I have received and understood you last transmission. It will be acted on where necessary
Say Again	Repeat your last transmission
Wait or Standby	Indicates that you are unable to reply immediately and is normally followed by an indication of time e.g Wait/Standby one means wait one minute
ETA	Estimated time of arrival
ETD	Estimated time of departure

**Phonetic
alphabet**

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

Numbers

0	Zero	4	For-wer	8	Ate
1	Wun	5	Fi – yiv	9	Niner
2	Too	6	Six	10	Wun - Zero
3	Thruh – ree	7	Seven		