



In association with  
**City & Guilds**

# **BIIAB Level 2 Award in Security Guarding Working as a Security Officer Unit**

## **Learner Materials**

Edition 2 – May 2011



## **BIIAB Level 2 Award in Security Guarding**

These learner support materials for the Working as a Security Officer Unit have been produced by BIIAB for use by BIIAB approved centres and the learners who attend training courses at these centres.

The learner support materials for the Working in the Private Security Unit and the Conflict Management for the Private Security Industry Unit can be found in the Award for Door Supervisors workbook available from BIIAB.

BIIAB approved centres are automatically licensed to use the learner support materials in any way that they wish including:

- Printing hard copies of the materials for use by learners
- Copying the electronic files on to CD to be sent to learners or to nominated tutors
- Using any part of the materials as handouts or as the basis for training slides

However, it should be noted that:

- Copyright on these materials remains with BIIAB
- The materials must not, under any circumstances, be circulated to non-BIIAB approved centres or any other Awarding Body
- The materials must not be reproduced in any way for sale

Any centre found to be in breach of these conditions will have their licence to use the materials revoked.

## Contents

1	The Role of a Security Officer within the Private Security Industry .....	5
1.1	The Main Objectives of a Security Officer.....	5
1.2	The Purpose of Assignment Instructions .....	7
1.3	A Security Officer's Equipment.....	7
1.4	Confidentiality .....	8
1.5	The Purpose of a Control Room .....	9
1.6	Activity .....	9
2	Patrolling.....	12
2.1	Types of Patrol and Their Purpose .....	12
2.2	Before Starting a Patrol.....	13
2.3	Patrolling Procedures and Techniques .....	14
2.4	Equipment Required for Patrolling .....	16
2.5	The Importance of Vigilance and Using Local and Site Knowledge When Patrolling .....	17
2.6	Activity .....	18
3	Access and Egress Control.....	20
3.1	The Purpose of Access and Egress Control.....	20
3.2	Types and Methods of Access and Egress Control.....	22
3.3	Statutory Agencies .....	26
4	Searching People and Their Property.....	28
4.1	Searching.....	28
4.2	Conditions That Have to be in Place Before Searching Can be Carried Out.....	28
4.3	Different Types of Search.....	29
4.4	Carrying Out Personal and Vehicle Searches .....	30
4.5	Refusal to be Searched.....	33
4.6	Documentation .....	34
4.7	Finding Property During a Search.....	34
5	Monitoring Systems.....	36
5.1	Types of Security and Monitoring Systems.....	36
5.2	The Functions of Electronic Security Systems.....	37
5.3	What Happens Next? .....	39
5.4	Alarm System Operator Controls and Indicators .....	40
5.5	Actions to Take in Response to Alarm Activations .....	41
5.6	False Alarms.....	41
5.7	Activity .....	42
6	The Law.....	44
6.1	The Importance of Knowing the Law.....	44
6.2	Relevant Legislation .....	44
6.3	Dealing With a Trespasser.....	47
6.4	Arrest Procedures.....	48
6.5	Reasonable Use of Force.....	49
6.6	Different Types of Evidence .....	50
6.7	Preservation of Evidence .....	51
6.8	Reporting Procedures Following a Crime .....	51
6.9	Activity .....	52
7	The Importance of Reporting and Record Keeping .....	55
7.1	The Different Types of Records Relevant to a Security Officer .....	55
7.2	The Do's and Don'ts of Report Writing.....	55
7.3	The Importance of an Incident Report.....	56
7.4	The Information to be Recorded in an Incident Report.....	57
7.5	Use of Pocket Notebooks.....	58
7.6	The Content and Importance of a Hand-Over.....	59
7.7	The NATO Phonetic Alphabet.....	59
7.8	Activity .....	61
8	Activity Answers .....	63

# 1 The Role of a Security Officer within the Private Security Industry

## By the end of this session

The learner will understand the role of a security officer within the private security industry and be able to:

- Identify the main objectives of a security officer
- Identify the purposes of assignment instructions
- List items of equipment needed when on duty
- Explain the term “confidentiality” within the context of a security officer’s responsibilities
- Identify the purposes of control rooms

## 1.1 The Main Objectives of a Security Officer

The chief role of anyone working as a member of security personnel is to deter and protect, which means that, regardless of the role that the person is carrying out, the preservation of life is primary with the protection of property being a secondary responsibility. With this in mind, the main objectives of a security officer can be summarised as follows:

Protection of life	Life threatening situations – fire, flood, chemical, gas leaks; slips, trips, falls; robbery, assault
Protection of property and premises	Burglary, theft, fire, flood, criminal damage
Prevention of loss and waste	Theft, breach of confidentiality, abuse of property
Prevention and detection of crime	Criminal damage, deception, theft, robbery, trespass, burglary, assault, public order offences

### ***Protection of Life***

This might be in specific situation, for example evacuation of premises following a fire alarm. It is also an important and ongoing role as part of a security officer’s normal duties in a variety of ways including:

- Monitoring of health and safety compliance (wearing of PPE)
- Reporting or dealing with maintenance requirements (slip hazards)
- Monitoring of alarm systems.

### ***Protection of Property and Premises***

This might be in a specific situation for example at a burglary, fire or flood situation. However, day-to-day functions such as monitoring of alarm systems, ensuring security equipment is working properly and vigilant patrolling all contribute to the protection of property and premises.

## ***Preventing loss and waste***

Loss can be suffered by an organisation in different ways:

- **Theft and other criminal activity** by staff, visitors etc. can be prevented or reduced by searching staff, visitors and vehicles in accordance with assignment instructions
- **Breach of confidentiality** whether intentional or not can have serious implications both to the organisation and the security officer. Confidential information should **never** be discussed with anyone including family and friends. The disclosure of confidential information could lead to criminal proceedings
- **Waste** through the unnecessary use of electrical equipment (lights, heaters etc) and the unauthorised use of telephone systems or computers. Security officers have a responsibility for waste management and measures to reduce wastage, which are required by environmental policies, may include activities such as switching of un-required electrical equipment, i.e. lighting, computers and machinery, if authorised to do so.

## ***Preventing Crime***

Within the security officer's area of responsibility there is the potential for many forms of crime to be committed, some more prevalent than others, depending on the type of site, for example:

- Robbery
- Burglary (break-ins)
- Criminal damage including graffiti
- Theft
- Deception
- Assault
- Breach of the peace
- Public order offences

Remembering that the main role of a security officer is to deter and protect, simply being seen can be a major help in preventing crime and other unlawful activity such as trespass. There are a number of ways in which this objective can be achieved including:

- Vigilant and comprehensive patrols, noting and reporting unusual activity, suspicious people, vehicles etc (the presence of an alert security officer acts as a major deterrent to most criminals)
- Implementing search procedures in accordance with assignment instructions
- Monitoring and responding to alarms, CCTV systems
- Controlling access to and exit from the site
- Ensuring security equipment is working properly e.g. security lighting.
- Reporting possible crime risks e.g. windows left open/pallets left by fence lines creating climbing frames etc
- Making suggestions to improve crime prevention measures.

## 1.2 The Purpose of Assignment Instructions

Assignment instructions are a reference manual containing information which is needed for security officers to carry out their duties effectively. They form part of the contract between the Customer and the Security Company, showing the customer's requirements.

Assignment instructions typically contain:

- Emergency contacts
- Emergency procedures
- Details of premises
- Duty objectives
- Reporting procedures
- Shift patterns
- Reporting for duty procedures
- Patrol details
- Responses to alarms
- Health and safety policies/risk assessments
- Search policies
- Access control requirements
- Equipment
- Radio procedures.

This list is not exhaustive and may be varied to meet the requirements of individual assignments.

Assignment instructions should be readily available.

As a security operative you have a responsibility to ensure that you are familiar with the content of the assignment instructions and to comply with their requirements. They should be checked at the commencement of each shift and any changes to instructions should be noted.

If you are unsure of, or need clarification on any of the content you should always **ask!**

## 1.3 A Security Officer's Equipment

To carry out your duty correctly and safely, it is essential that a security officer has the correct equipment and it is the responsibility of each officer to ensure that the equipment issued is working correctly and in good condition at the start and end of each duty.

The following equipment should be on all assignments:

- Assignment instructions
- Daily occurrence book
- Other reports/registers e.g. key registers and visitors book
- Keys
- Torch.

Dependant on the type of assignment there will be additional equipment, which should be shown in the assignment instructions.

This will include some or all of the following patrol equipment:

- Clocking device
- Swipe card
- Communication equipment e.g. a radio or a telephone
- Pocket book and pen
- Pager.

Officers will also have Personal Protective Equipment (PPE) in addition to the above, which may include:

- High visibility clothing
- Protective footwear
- Hard hats
- Eye protection
- Protective gloves
- Ear defenders
- Wet weather clothing.

## 1.4 Confidentiality

The security officer has access to confidential information and is trusted and required to maintain the confidentiality of that information. Types of information include:

- Employee information
- Client information
- Sensitive company documents
- Security procedures
- Location of detection equipment
- Alarm codes.

Security officers must make every effort not to reveal any connection between their personal circumstances and their work. Consider the effects of wearing work uniform or high visibility clothing out of work. This clearly identifies your role and responsibilities and may be all the invitation that a criminal needs to approach you an attempt to extract confidential information.

If a security officer is approached for information from an unauthorised person (either on or off duty) this approach should be reported.

Confidential information should only be disclosed to authorised personnel and **never** to friends, family or customers.

**REMEMBER** - unauthorised disclosure of confidential information by a security officer can have serious consequences not only for the organisation, but the security officer too, as they could be the subject of criminal proceedings.



## 1.5 The Purpose of a Control Room

The control room is the 'nerve centre' of a security operation and any incident, activity or change in circumstances affecting the safety of individuals, the security of the site and the day-to-day running of the security operation should be reported to the control room promptly. For example, the security officer must keep the control room informed of changes in their availability for duty (late for duty, sickness etc) as soon as possible to ensure the assignment is properly covered.

The Control Room Officer:

- Provides emergency support and back up to security officers on duty
- Assists with enquiries
- Monitors the security officers' safety with check calls
- Plans the site coverage by co-ordination of security officers' activities
- Monitors radio and other communications
- Monitors CCTV and alarm systems.

## 1.6 Activity

Without looking at your notes try to complete the following activities:

1. What is the most important objective of a security officer?
2. What are the main roles and responsibilities of a security officer (Four P's)?
3. An organisation can suffer loss in a number of ways including breach of confidentiality – identify two other ways loss can be caused, giving an example for each.
4. Identify five types of crime the security officer needs to be aware of.
5. You are sent to a new assignment and want to familiarise yourself with the site. Highlight the five items from the following which you would **not** expect to find in the assignment instructions.
  - Emergency contacts
  - Emergency procedures
  - Details of premises
  - Duty objectives
  - Reporting procedures
  - Shift patterns
  - Reporting for duty procedures
  - Patrol details
  - Responses to alarms
  - Health and safety policies/risk assessments
  - Search policies
  - Access control requirements
  - Equipment
  - Radio procedures
  - Details of overtime rates

- Holiday entitlement for security staff
  - Security officer's personal details
  - Training records
  - Grievance procedures.
6. Where would you expect to find information on responses to alarms?
- A In the managers log
  - B In the incident report
  - C In the health and safety manual
  - D In the assignment instructions
7. Which of these would you **not** expect to find in the assignment instructions?
- A Radio procedures
  - B Overtime rates
  - C Patrol Procedures
  - D Shift Patterns
8. Which statement most accurately describes the main purpose of assignment instructions?
- A To ensure security officers know their rights in case of a dispute
  - B To record details of an incident on a site when the emergency services are called
  - C To act as a reference manual for security officers which contains information essential to their duties.
  - D To assist supervisors in ensuring the site is covered properly
9. List four items of Personal Protective Equipment (PPE) you may need on an assignment.
10. In addition to PPE, list four other items you should have with you on a patrol.
11. List six types of confidential information the security officer may have access to.
12. You are in the control room and receive a telephone call. The caller is reluctant to identify themselves but says they are a friend of a security guard and could you give them the security officer's home address. You should:
- A Give the details but tell the security officer concerned what you've done
  - B Not give the information as it is not immediately to hand but tell the caller when the security guard is next on duty
  - C Give the information as there's no harm in doing so and part of your job is to be helpful to the public
  - D Not give the information as it is confidential, try to identify the caller and inform your supervisor.
13. It's your day off. In a seemingly innocent conversation an acquaintance asks you how many security guards cover your site on a night shift. You should:
- A Give them the information and think nothing more of it
  - B Give them the information but tell them it's confidential
  - C Give a fictitious figure

D Not give any information and advise your supervisor

14. List five functions of a control room officer.

15. Answer true or false for the following five statements:

- A A control room is an area where security officers should get together to have meetings
- B Part of a control rooms' role is to monitor activity of security officers
- C Any incidents happening whilst you are on duty should be reported to the control room promptly
- D Monitoring of alarm systems is an important function of a control room
- E A main purpose of a control room is for security officers to store their equipment

## 2 Patrolling

### By the end of this session

The learner will understand the importance of, and reasons for, patrolling and will be able to:

- Identify the types and purposes of different patrols
- Identify actions that should be taken before starting a patrol
- Describe patrolling procedures and techniques
- State the equipment required for patrolling
- Explain the importance of vigilance and using local and site knowledge when patrolling

### 2.1 Types of Patrol and Their Purpose

Security patrols may take place internally (inside offices, factories, laboratories, warehouses etc), externally (outside buildings, around secure perimeters, around open grounds, car parks etc) or varying degrees of both. It is important that the security officer stays vigilant during these patrols reacting to and reporting all suspicious or unusual discoveries.

There are four types of security patrol with variations affecting procedure at the start and ends of the shift:

1. The initial patrol i.e. the first patrol of the shift. If your initial patrol coincides with the site closing down at the end of their business day, then this patrol is known as a 'Shut down' patrol. Whereas if your initial patrol coincides with the site opening up for business, then this patrol is now called the 'Unlock' patrol.
2. The subsequent or interim patrol
3. The specific patrol
4. The final/last patrol which is also subject to how the site business is operated and will be known as either the 'Shut down' or 'Unlock' patrol

#### ***The initial patrol***

The initial patrol is the first patrol of the shift. This patrol enables the security officer to ascertain the status and condition of their site and sets a 'bench mark' from which a Security Officer will easily be able to identify any change and become alerted to possible unlawful activity.

If the initial patrol is to achieve a 'Shut Down' it should be the longest and most detailed of that shift's patrols. It is during this patrol that insecure doors, open windows, and unlocked gates are most likely to be discovered as well as running taps and switched on lights and electrical appliances.

All such discoveries should be put right, reported and recorded – none of the above should be discovered on subsequent patrols.

It is during the initial patrol that the security officer's areas of responsibility are locked down, secured and made safe.

### ***Subsequent or interim patrols***

Subsequent or interim patrols ensure that any change in the state of the site from the initial patrol is discovered and reacted to in a timely and professional manner.

The amount, duration, routes and timings of the interim patrols will be stated in the site's assignment instructions

Interim patrols may be at regular intervals or random depending on the policy and procedures of the site. Regular patrols ensure that a set amount can be achieved over a shift. However, carrying out random patrols is considered to be good practice to prevent criminals from learning patrolling patterns and taking advantage of these. For the same reason, route times, patterns and directions should vary.

### ***Specific patrols***

Specific – sometimes known as Snap – patrols are carried out on high risk areas and/or areas where a security weakness has been identified. Areas with insufficient lighting, bad CCTV coverage, alarm system failure, or prime targets for criminal activity will be covered by specific patrols. The location and frequency of specific patrols will change on the same site over subsequent shifts. This is because identified risks will usually be short term and change as they become resolved and new risks are discovered. It is important that the security officer familiarises themselves with their site instructions at the beginning of every shift.

### ***The final/last patrol***

The last or final patrol is the last scheduled patrol carried out on shift as opposed to the last patrol carried out. This patrol may be a locking or unlocking patrol, depending on the site's assignment instructions. As this is the last check made before handing over to the next shift, it is imperative that the next shift's initial patrol does not discover any unreported irregularities. Unreported and/or unresolved discoveries made by the next shift, that should have been dealt with by the previous shift, will reflect badly on everyone involved in the delivery of the security services.

## **2.2 Before Starting a Patrol**

It is important at the start of their shift that the security officer familiarises themselves with the site's assignment instructions. These instructions should also contain any specific tasks relating to that shift including the number and frequency of patrols, areas requiring specific patrols and any health and safety issues that the patrolling officer should be aware of when patrolling the site.

It is imperative that the site assignment instructions and handover points are understood before commencing a security patrol.

Before starting a patrol:

- Secure your base and use a land-line telephone to inform the control room that you about to undertake a patrol
- Ensure that their equipment is working – alarm systems, CCTV etc.
- Ascertain if there any areas of concern they need you to check out during your patrol
- Check that all your equipment needed during the patrol is in working order

- Make a radio check call with your control room to ensure that your prime means of communication is fully effective. Always use proper call signs and remember confidentiality rules to guard against unlawful signal monitoring activity
- Log the start time of the patrol in the daily occurrence log (and your pocket notebook)
- Ensure that all unnecessary lights and electrical appliances are switched off
- Ensure that any other health and safety instructions specific to the site are complied with (including the wearing of PPE)
- If your radio signals are secure inform the control room that you have started your patrol
- Secure the security base area.

### **2.3 Patrolling Procedures and Techniques**

A security officer has four priorities all of which must be exercised when on patrol in the following order:

1. Preserve their own health and safety
2. Preserve the health and safety of others
3. Preserve the integrity of the site
4. Prevent loss or damage.

It is important that the order of these priorities is not confused during a patrol.

Section 44 of the Employment Rights Act 1996 indicates that staff have the right to remove themselves from their place of work if they assess that there is a real and present danger to their wellbeing. Therefore, security officers must not allow themselves to knowingly place themselves in a dangerous situation by, for example, walking into burning buildings, confronting armed criminals, scaling perimeters or walls in pursuit of intruders, etc.

Whilst taking full regard for your own health and safety, it is also important to prevent others from attempting to place themselves in a dangerous situation as described in the examples above.

By preserving the integrity of the site and maintaining a highly visible and professional presence, loss should be prevented.

#### ***Internal patrols***

Before entering any building ensure that it is safe to do so. If practicable, a full 360 degree external patrol of the building should be carried out before entering to check whether there are:

- Smoke or flames coming from the building
- Any signs of forced entry
- Any unusual lights, shadows or noises.

If the answer is yes to any of these security officers should perform a dynamic risk assessment, keep a safe distance away and inform the control room. Details of how to deal with intruders or fire will be in the assignment instructions.

Take a note of any open windows, visible lights left on, defective external lights, etc.

When you are confident it is safe to do so enter the building. As with the external patrol of the building, beware of signs of intruders and fire as you progress.

A patrol of a building involves checking the building's status, not just walking through it. Therefore, a security officer must:

- Check all internal doors and windows are shut – this prevents unlawful access and the spread of fire.
- Neutralise and report any fire hazards – heaters next to combustible materials, highly flammable materials incorrectly stored, missing fire extinguishers, blocked or propped open fire exits, cigarette butts and smoking materials, etc.
- Turn off and report any running or dripping taps if authorised to do so. (e.g. laboratories may require water supplies to be continuous)
- Make safe and report any slip, trip or fall hazards and/or any unsafe storage practices
- Ensure and report that all unnecessary lights and electrical appliances, and machinery is switched off – your assignment instructions will state what has to be left on.
- Check toilets, kitchens, wash and shower rooms etc for unconscious or unauthorised personnel as well as leaks and water damage
- Check that all internal security and safety equipment is functional and has not been tampered with, for example:
  - Are the static CCTV cameras pointing in the correct direction?
  - Is the camera's view obstructed?
  - Are the internal security alarms working and unobstructed?
  - Is the fire alarm panel switch on and working, or is it de-activated or in fault?
  - Do the fire alarm sensors appear to be in proper working order or are they damaged or tampered with?
  - What was the security alarm status of the building when you entered?
  - Can all the systems in the building be fully activated before you leave the building?
  - Can the building be locked when you leave?

A pocket notebook entry should be used to record the status of the building, your actions, and anything discovered that is unusual, suspicious or hazardous. It is also good practice to record when you entered and secured the building, making a note that the systems were seen to be working correctly when checked on your patrol. This information is invaluable for subsequent patrols and will highlight any changes that occurred between patrols. The information may also require entering in a Daily Occurrence Book or as a specific Incident Report.

### ***External Patrols***

Always be vigilant when undertaking external patrols – take extreme caution when approaching unlit areas and if possible have your control room follow you on CCTV. A secure site should have adequate external lighting so any areas that are inadequately lit should be reported as both a security and health and safety risk.

Inform the control room when locking or unlocking gates, barriers, and doors. As with unlit areas have them follow you on CCTV. Beware of vehicles and people which cause you to be suspicious.

Carrying out external patrols mean that you will be exposed to the weather – ensure that you are dressed correctly and take extreme caution during high winds.

An external patrol is carried out to ensure that the site's perimeter and grounds are safe and secure.

When undertaking an external patrol, check that all external security and safety equipment is fully functional, for example:

- Are the static CCTV cameras pointing in the correct direction?
- Are the pan, tilt and zoom (PTZ) CCTV cameras reacting correctly?
- Are any of the external cameras' views obstructed?
- Are the perimeter alarm systems damaged – do they look as if they have been tampered with?
- Are all of the exterior lights working?
- Are there any signs of intrusion – holes in fences, climbing aids, etc?
- Are there any breaches of fire and health and safety regulations – slip, trip or fall hazards, unsafe storage practices, running taps, blocked fire exits and emergency access points etc?

As with internal patrols – record all of your findings in your pocket notebook.

### ***On completion of the patrol***

- Inform the control room – or whomever stated in the assignment instructions – that the patrol has been completed
- Complete the daily occurrence book and/or any reports from the details recorded in your pocket notebook.

## **2.4 Equipment Required for Patrolling**

Before carrying out a patrol you must check that all your equipment needed during the patrol is in working order. Some equipment may be site specific but listed below are the usual requirements. All necessary equipment will be listed in the assignment instructions.

- **Torch** – a torch is essential for effective patrolling. It allows the security officer to see and be seen. It can also be used as a signalling device to alert and direct the emergency service
- **Radio** – a radio is your prime means of communication with the control room and fellow officers (this may be supplemented or replaced with a mobile telephone). Some radios are equipped with a lone worker function that alerts the control room if the patrol officer becomes unconscious by sending out a signal if the radio remains stationary for a set period of time
- **Keys and/or access card** – keys are signed out and back in by the security officer at the beginning and the end of every shift. The security officer is responsible for them and they should be carried on the security officer's person at all times
- **Pocket notebook and pen** – a security officer is responsible for their own pocket notebook. Officers should ensure the security of their notebooks and its contents and must adhere to any archiving policies adopted by their employers. Pocket notebooks may be used to aid official investigations and may be subject to seizure by enforcement agencies such as the Police or Revenue and Customs. Entries must not be removed or erased. It is good practice to use a black ball point pen – a fountain pen will leak and run in wet weather, blue ink is difficult to photocopy, and pencil can be erased. Missing notebooks should be reported
- **Personal Protective Equipment (PPE)** – the level of PPE required will differ, depending on your site's assignment instructions. If your patrol requires you to enter



areas controlled by mandatory PPE signs you must comply no matter what time of day the patrol takes place. The following are examples of PPE that you may be required to wear:

- High visibility clothing
  - Hard hat
  - Eye protection
  - Protective footwear
  - Protective gloves
  - Ear defenders
  - Wet weather clothing
- **Landline telephone** – access to a landline telephone may be necessary because of radio blind spots or other interference. It may also be necessary for the security officer to contact the emergency services directly rather than through their control room.
  - **Clocking device** – an electronic device that reads and records the time and location of set of clocking points around the site. This is used to prove that the security officer performed their set patrols and covered the areas required. Clocking points are usually located in key areas – high hazard, high values, high risk etc.

## **2.5 The Importance of Vigilance and Using Local and Site Knowledge When Patrolling**

Vigilance, observation, curiosity and a suspicious nature enable a security officer to carry out their patrols safely and effectively and enable them to quickly identify anything that could put themselves or the site at risk.

A security officer should never take anything at face value or for granted and, when patrolling should use all of their senses – not just sight and hearing, for example:

- Before opening a door touch it to feel if it is hot – there may be a fire on the other side
- Smell the air – is it damp (water damage?), smokey (fire?), sweat or cologne (someone else in the room?), acidic (spilt chemicals?)
- When entering a building or room is it unusually hot (fire?) or cold (open window or door?)

You should never place yourself in danger; if a potentially dangerous situation arises always get help and do not attempt to tackle the situation alone.

For a security officer to be fully effective they should have a good local and site knowledge. This will enable them to quickly identify any vulnerable areas and to react quickly to any incidents that might arise.

### ***Local knowledge:***

- Is the site situated in an industrial or residential area?
- What are the working patterns of the neighbouring businesses?
- What time are deliveries usually carried out – when would you expect to see vehicles in the area?
- Do people usually walk or drive past the site outside of normal working hours – is it a regular throughway?

- What is the local crime rate?
- Is there local opposition to your site?
- Are the buildings adjacent to your site easily assessable?
- From which direction would the emergency services come from when called?
- How far away would they come from?
- How often do the police patrol the area?
- What is their response time?

**Site knowledge:**

- Where are the emergency access points?
- Where are the emergency assembly points?
- What hours are the premises open from and to?
- Is there occasional late or early working?
- What areas are covered by the CCTV system?
- What areas are not covered by CCTV?
- Where are the emergency exits, assembly points and call points?
- Where are the security alarm panels?
- Are there any dangerous substances on the premises?
- Is there any work considered to be of a dangerous nature being carried out that might affect security or health and safety? Are all practices and procedures being carried out in accordance with relevant Health and Safety legislation and in accordance with any risk assessments?
- Where are telephones located around the site?
- Are there any points that could be used for unauthorised access?
- What are the most vulnerable areas on the site?
- What areas would be targeted by intruders with criminal intent?
- Where is your escape route if confronted?

***If security is found to be breached***

The professional security officer will ensure that they have read and understood their assignment instructions. If security is found to be breached the security officer should follow those instructions – ensuring that their health and safety is maintained at all times, for example:

- Inform the control room and any other relevant persons
- Secure the area
- Preserve the evidence.

Ensure that the security of the site is re-established as soon as it is practicable to do so.

**2.6 Activity**

Without looking back at your notes, try to answer the following questions.

1. List the four types of patrol
2. During which patrol should the security officer ensure that their areas of responsibility are locked down, secured and made safe?

3. List three duties that need to be carried out before starting a patrol
4. What are the security officer's four priorities when on patrol?
5. Give three indications that it may be unsafe to enter a building?
6. Where should you record any anomalies or occurrences that are noticed on patrol?
7. List three types of equipment needed for a patrol
8. Name the two types of knowledge needed by a security officer?
9. What **must** the security officer do if security is breached?

## **3 Access and Egress Control**

### **By the end of this session**

The learner will understand how to control access to and egress from a site and will be able to:

- Identify the purposes of access and egress control
- Identify duties of a security officer when using different methods of access and egress control
- State the powers and identification requirements of statutory agencies

### **3.1 The Purpose of Access and Egress Control**

Access and Egress Control means that there is a system in operation that controls who or what can enter or leave a site lawfully. The access control system used will depend on the site's location and the perceived risks associated with that site. Professionally controlled access and egress will enable all concerned parties, including security, management, health and safety, and the emergency services, to have an accurate record of who is on and off site at any given time.

Unrestricted access or un-enforced access control provides those with criminal intent the opportunity to gain access to unauthorised areas. If the opportunity is provided they will take it!

Maintaining control of the access and egress to premises reduces the risk of criminal or dangerous acts occurring on those premises.

Access and egress control is one of the primary and most highly profiled duties of a security officer. The security officer will need to be able to deal with the general public and operate various methods of controlling site access and egress to enable authorised access and egress and prevent unauthorised access and egress.

To meet this requirement the security officer needs to know who is and who is not authorised. This information will be in the site's assignment instructions. The security officer must familiarise themselves with this information before taking on the responsibilities associated with enforcing access and egress control.

Access and egress control will apply to the following:

- Current employees
- Notified visitors
- Authorised contractors
- Authorised cleaners
- Notified/authorised couriers
- Representatives from statutory agencies.

All of the above will report to the premises' entry points and will be reliant on the duty security officer and/or the security entry systems to allow them access and egress. However, there are other people who may attempt to gain unauthorised access or egress. Security officers must be constantly aware of this potential. They must do all they can to

deter, detect and report such activity. People attempting to gain unauthorised access will possibly include the following:

- People with criminal intent
- Ex-employees who may demonstrate animosity or be bared from entering due to their previous actions. This may pose a particular problem if the ex-employee now has a job that would usually allow site entry; i.e. delivery driver
- Angry neighbours or persons disgruntled with the company or one of its employees
- Vagrants
- TV and newspaper reporters.

It is important that when carrying out their duties and dealing with the general public the security officer must be professional, courteous, and mindful of their health and safety at all times.

### ***Unauthorised Access***

For access control to be effective the security officer must be able to detect unauthorised access. The security officer should be observant and suspicious at all times and be aware of the following indicators:

Physical:

- Activated security alarms
- Broken or open windows
- Damaged or open doors
- Ladders or other climbing equipment left unattended
- Noises
- CCTV.

Behavioural:

- Walking or running away when being approached
- Hiding or attempting to conceal themselves
- Attempting to hide something they are carrying
- Location - being in an unauthorised area
- Being inappropriately dress for the area they are found in – no PPE, no company issued clothing etc
- Unacceptable answers to your questions
- Being uncooperative
- Not having a visitors or employees pass.

When unauthorised access is discovered the security officer must follow the assignment instructions, report it, get help, and ensure that their health and safety is observed at all times.

## 3.2 Types and Methods of Access and Egress Control

To assist security services to provide effective access and egress control procedures, equipment has been developed which allows proven types and methods to be adapted and adopted according to site needs. The equipment falls into two categories; 'Mechanical' or 'Electrical' as shown below.

Access control will be located at various points around the premises. These will be as follows:

- The premises' external entry points e.g. gatehouse, reception, car park etc.
- Secure storage areas
- Vulnerable or high risk areas
- Remote entrances
- Restricted areas.

The type of access control used will depend on the relative cost, the risk, the maintenance, the control, and its practicality. For example, biometric access reading equipment is used to identify an individual person by reading the retina of their eye or their fingerprint and so biometric access readers are unlikely to be used on a remote gate that is only opened once a year when a simple chain and padlock would suffice. Depending on the customer's needs the security officer will be trained to be competent in operating the adopted system.

### **Mechanical** – *manually operated by the security officer*

#### Locks

Shutters Can be manual or electric operation. Manual shutters are operated via cord, geared winding handles or spring & lock operation. Electric security shutters can be remote controlled or hard wired. Electric security shutters can be controlled individually or in a group dependent on situation.

Gates There are numerous types of security gate some of which are to control access and egress of people and others of vehicles. Different gate types include swinging gates, sliding gates and bi-folding gates. Gates can be opened manually or may be powered by electricity

Barriers Used to control the access and egress of vehicles and can be either manually or electronically operated.

Turnstiles Turnstiles are used to control access and egress of people. They can be half height, ¾ height or full height and allow the security officer to restrict entry an exit as necessary

Rising kerbs These are used to prevent vehicular entry into both manned and unmanned areas. They are available in a variety of heights and widths so that maximum security can be achieved as required. Operated using hydraulics, they can be lowered or raised to permit or prevent access or egress as required.

### **Electrical** – *automatically controlled by a programmed system*

Electronic locks An electronic lock is a lock which operates by means of electric current. Although these can stand-alone, with an electronic control assembly mounted directly to the lock, they are more commonly connected to an access control system. The advantages a system of this kind includes key control (keys can be added and removed without

re-keying the lock cylinder) and transaction logging, where (entry and egress activity is recorded).

Keypad systems	Locks that are operated by keying in a specific code
Swipe cards	Swipe cards are a low-cost, flexible, easily maintained means of controlling entry to and exit from premises. Card readers can be fitted to many different internal and external doors and to other entry points, such as gates and barriers. Every card is individual, allowing restricted access to, for example, computer server rooms, and many systems can automatically record who went where and when. For the reader to read the card, the magnetic strip on the card must be passed through the reader.
Proximity readers	Proximity readers use contactless technology. They are a robust, low-cost, highly secure way for to control access and egress. Individual identification and access policy data, along with the operational technology, are securely stored within a contactless integrated circuit device, such as a card or fob, reducing the likelihood of damage or copying. As with a swipe card system, proximity readers can be fitted to both internal and external entry and exit points and can record people's movements if required.
Biometric readers	Biometric readers are a highly secure means of verifying people entering and leaving a site. They allow entry only if the authorised user's unique human characteristics are recognised. They also remove the administrative difficulties caused by people forgetting or losing their card, or clocking each other in and out. Biometric readers electronically store a template of certain physical characteristics in an electronic memory and then automatically authenticate these when the person enters or leaves a building. Geometric fingerprint patterns are most commonly used but others are available including retina, iris, hand, face or fingerprint matching, and voice recognition.
ANPR – Automatic Number Plate Recognition	APNR technology monitors and captures number plate images and these camera control systems are designed to: <ul style="list-style-type: none"><li>• Monitor unauthorised use of parking areas</li><li>• Monitor vehicle movements</li><li>• Enforce limited waiting regimes</li><li>• Generate revenue</li></ul>

The location, description, and instructions for use of these systems will be in the site's assignment instructions. The security officer must familiarise themselves with this information.

### ***Access Control at Gatehouses***

The security gatehouse is usually the first point of access for visitors to a site. The security officer stationed at the gatehouse will have to deal with two types of access – pedestrian and vehicles.

### ***Passes***

The security officer stationed at the gatehouse will check employees' passes and issue temporary passes to visitors and contractors.

The security officer must ensure that all temporary passes are accounted for – signed out and returned on exit.

The type and design of the pass depends on the client's needs and preferences:

### ***Employee's Passes***

Employee's passes may double as an access control card, which is usually a card designed like a credit card size and used to operate an electronically controlled system, by either swiping it through or holding it against a 'sensor' reader.

They usually state the employees name and department, and have a current photograph for visual identification. To gain entry the passes must be clearly displayed to allow the security officer to confirm access rights. The security officer should also be able to check that the pass is current – not expired, correct for the level of access required, genuine – not a forgery, and actually belongs to the person using it – name and photograph

### ***Temporary Passes***

Temporary passes should be worn in plain sight by the person it is issued to at all times whilst on the premises. Ideally the pass should display the visitor's name, company and contact. This pass should be returned to the security officer every time the person leaves the area to which access is approved. It is the responsibility of the security officer to ensure that all temporary passes are accounted for. If passes cannot be accounted for the security officer should contact the host person they were visiting to check whether or not that person is still on site or if they have left with a pass by mistake. The visitor's log should be updated accordingly if the visitor has left. Some sites or part of sites require visitors to be escorted to meetings etc.

### ***Visitors' Logs***

One of the prime duties of a security officer stationed in a gatehouse or reception area is to maintain a visitors' log. This log may be electronic but many are still hand written and should be completed at the time as this prevents belated or fraudulent entries being made after an incident.

The visitors' entry log is a very important piece of documentation. It is a record of who is currently on the premises and why. It can be used as an assembly register during an evacuation and it may be required as evidence by third parties post incident. All details entered in the log must be accurate, legible, and complete.

A completed entry will usually show the following information:

- The visitor's name and company
- Purpose of visit
- Host or escort – person being visited
- Date and time of arrival
- Time of departure
- Details of pass issued – level of access, pass number etc
- Vehicle registration number.



### ***Infringements and Faults***

Any problems concerning the effectiveness of the access control system or infringements by members of staff or visitors must be reported and recorded in the daily occurrence book.

## **Vehicles**

The access of vehicles can be physically controlled by the security officer using one of the following methods:

- Gates
- Barriers
- Lights
- Raised Kerbs – or bollards.

The security officer must be satisfied that any vehicle, equipment or goods it is carrying, vehicles and all of its occupants have authorisation to enter the premises. This means that they all have to be accounted for – driver, passengers, goods etc.

The security officer, depending on their assignment instructions, will be responsible for:

- Controlling and allocating visitor passes
- Controlling and allocating vehicle passes
- Issuing maps or directions
- Giving verbal directions
- Informing them of the speed limit and allocated parking areas, as well as any other health and safety related instructions.

The assignment instructions may require vehicles to be searched before entering or leaving the site or any part of the site – the security officer performing this task should be professional, polite, observant, and aware of their health and safety throughout.

**Remember: during a major incident the emergency services will require unimpeded access to the premises. It is the security officer's responsibility to ensure that emergency access points are kept clear and that vehicles do not cause obstructions!**

### **3.3 Statutory Agencies**

Visitors from statutory agencies have the legal right to enter any premises where they are authorised to carry out their inspections. They will provide identification and documentation that states who they are and why they need access.

Visitors from statutory agencies include:

- Health and Safety Inspectors
- Factory Inspectors
- Environmental Health Officers
- HM Revenue & Customs Officers
- Fire Safety Inspectors
- Police in possession of a warrant
- SIA investigators and those with written authority
- A police officer who is in the immediate pursuit of an offender or person at large; i.e. an escaped prisoner or someone in breach of a warrant

They **cannot** be refused entry, but it is the security officer's duty to ensure that they are informed of any health and safety issues before they enter.

Statutory agencies do not have to give advance notice of their visit, which can take place on any day and at any time.

The security officer's assignment instructions will state who must be informed when visitors from statutory agencies arrive.

Statutory agencies have various rights which include the right to:

- Copy and remove documents without the customer's permission
- Take photographs
- Take statements from anyone on the premises
- Cordon off or close down areas or all of the premises
- Issue an improvement notice.

The security officer must give their full cooperation and not hinder them in any way.

## 4 Searching People and Their Property

### By the end of this session

The learner will understand basic search procedures and will be able to:

- List the conditions that have to be in place before searching can be carried out
- Identify the different types of search
- State the correct procedures for carrying out personal and vehicle searches
- State actions to be taken in the event of a refusal to be searched
- State the information to be recorded in search documentation
- State the action to be taken when property is found during a search

### 4.1 Searching

To deter criminal activity and protect property and assets, the security officer will be expected to carry out searches of people and their property. Depending on the nature of the assignment and the customer's requirements 'people' may include:

- Employees
- Contractors
- Customers
- Delivery drivers
- Visitors
- Security officers.

Their property may consist of vehicles, lockers, desks, filing cabinets, bags, clothing, or any personal belonging they have on company premises or wish to bring on to company premises.

Depending on the nature of the site these searches may occur before entry to site, before leaving site, whilst on site, or combination of all three.

### 4.2 Conditions that have to be in place before searching can be carried out

Before any searching can be carried out at your assignment on any person or their property the person is legally required to meet specific conditions, the most important of which is that the person **must** give permission for the search to take place. Other conditions may include the following:

- An employee or their property is not subject to search on entry to, exit from, or at any location on company premises unless it has been agreed as part of their conditions of employment. This may include an agreement with the employees union
- Notices must be prominently displayed for visitors and they should be verbally informed about the search, and agree to it, before entry. If the visitor does not agree to the search they can be refused access
- Contracted companies agree to their employees and property being searched as part of the contractible agreement with your customer
- The security company's service contract with the customer must state that searching of people and property is part of the service agreement and what this searching entails

- All searches must be witnessed and recorded
- No search can be carried out without first obtaining the person's permission – before each search
- Security officers have no special rights in relation to searching people and their property
- They cannot use force, threat or deception to obtain a search. The reason for the search must be stated and permission to carry out the search must be clearly asked before it can take place
- Even after initially agreeing to the search, the person being searched, can stop the search from continuing at any time during the search if they change their mind
- Agreement to search in conditions of employment, contract, or on entry to site does not negate the need for permission to be given before any search can be carried out.

**If these conditions are not complied with and the security officer carries out a search on the person, or their property, without the person's permission the security officer can be accused of committing assault.**

The assignment instructions will give all of the relevant details regarding search:

- When and where searches are to be carried out
- What type of search is to be carried out at which location and time
- What the local company or departmental rules are concerning searching
- What to do and who to contact if any problems are encountered.

### **4.3 Different Types of Search**

There are several types and methods of search:

#### ***Personal***

- Metal Detector Arch – mainly used at airports to detect weapons
- Hand Held Metal Detector – used at airports, prisons, high security installations to detect weapons or industrial sites on egress to detect theft.
- Hands on Search – to complement the above or to detect non-metallic items such as illegal drugs. Hands on searching is often carried out at venues where both concealed weapons and drugs are a known problem.

#### ***Personal Property***

- Vehicles – on entry to and exit from site
- Lockers or personal storage areas – these searches usually require the owner or an approved representative to be present.
- Bags and other carried items – including mail, sealed units, and items carried on the behalf of a third party
- Desks and filing cabinets – as with lockers these should be carried out in the presence of the owner or an approved representative.

#### ***Other***

- Rummages – searches of possible hiding places such as toilets, offices, machinery, storage areas etc, usually carried out as part of a patrol
- Laundry – on entry or exit depending on the security needs of the assignment
- Rubbish – visually, on sorting tables and/or with x-ray machines.

These searches can be either random or specific.

### ***Random Searches***

Random searches are used as a deterrent especially where resources cannot maintain 100% searching.

Random personnel or vehicle searching may involve either an electronic selector or an agreed system – every other person or fourth person is not random. The security officer must adhere to the system to ensure against accusations of harassment or victimisation.

A security officer may override the system or selector if they feel they have justifiable cause e.g. someone acting suspiciously. This then becomes a Specific Search.

### ***Specific Searches***

Specific searches are usually carried out as the result of information or evidence relating to security incidents and will involve searching specific people or even a single individual.

This information or evidence may be obtained by observations on CCTV, observations made by a security officer, or observations reported by a third party. Consideration must be given to the 'source' of the information and associated credibility.

Equally, the information or evidence may be obtained by the results of an ongoing investigation or as a need to confirm any reasonable suspicions.

Random and specific searches must be carried out with due care to the security officer's health and safety. The security officer must ensure that their assignment instructions and procedures are adhered to, that all necessary paperwork is correct and that any evidence is preserved.

## **4.4 Carrying Out Personal and Vehicle Searches**

As previously stated a search **cannot** be carried out on a person or their property without that person's permission. A person's property is legally seen as an extension of themselves so any search carried out on a person's vehicle, baggage, clothing, etc will be classed as assault unless permission to search is given.

### ***Personal Search***

Personal searches should be carried out in designated or private areas which are fit for purpose, being free from danger (exit routes and appropriate furniture), and provide the required privacy for the person being searched (curtains or blinds) .

Designated areas should display appropriate signage to identify that the areas are approved and, for the protection and safety of all concerned, should be covered by CCTV. Any searches carried out in private areas should be conducted with an independent witness present.

Before carrying out a search, the security officer must ensure that the person is aware that a search is about to be carried out and the reason for the search. Remembering that the security officer must then obtain the person's permission before undertaking the search, best practise advises that the person being searched also signs a search register to confirm

that permission has been given. If the person refuses to sign, this should be recorded by the officer and endorsed by any witnesses.

The security officer must be polite and courteous at all times, from beginning to end. Some people are uncomfortable being searched; they may see it as an invasion of their privacy or their personal space. They may consider the search as an indication that they are not trusted or perceived as dishonest. They may have a problem with authority and harbour resentment towards you or the company you represent. They may simply feel embarrassed by the situation.

Under any of the above circumstances the person being searched may react out of character. Security Officers should remain positive, assertive, alert and take nothing for granted but not assume that the person's reactions are proof that they have something to hide.

The behaviour and actions of the security officer during the search will affect the behaviour and actions of the person being searched:

- Be sensitive to the person's feelings – awkwardness, embarrassment, aggression etc
- Do not mock, ridicule or be rude to the person as this may be seen as degrading or humiliating and be ruled as a breach of the individual's Human Rights
- Be tactful and understanding
- Be assertive and firm, but consistent and polite
- Be aware that you are seen as a representative of authority and may be perceived as threatening
- Do not take their reactions as a personal insult it is because of the situation not you.

By remaining polite, positive, and professional throughout the process and adhering to the set down procedures the officer will hopefully get full co-operation and not be accused of victimisation or harassment.

It is unprofessional to select people for search because of their gender, ethnic background, religion, dress, appearance, or status – to do so would be victimisation. It is also unprofessional to deliberately not select people for the same reasons on the grounds that you wish to avoid accusations of victimisation. A security officer must conduct their duties in an unbiased professional manner at all times to ensure that search is an effective deterrent and security is maintained.

### ***Searching the opposite sex***

Depending on the assignment instructions, it is the usual for men to only search men and women to only search women. Deferent assignments may have variations on who is allowed to search whom – with hand held metal detectors for example – but males should not physically touch females and females should not touch males.

A male officer may search a woman's bag or belongings – with the woman's consent but to avoid causing embarrassment it is better to let that task be undertaken by a female officer. Likewise a man may feel uncomfortable about a woman searching his locker or briefcase because he is embarrassed or he feels that the female officer would be embarrassed by what she found.

### ***Searching personal effects***

All searching must be conducted in plain sight, and witnessed by a third party or under CCTV:

- Do not put your hand in pockets, bags, wallets or purses: ask the owner of the items to open and/or empty them
- If the owner gives you permission to take something out of their pocket or bag: don't do it. Never let yourself be coerced into being accused of planting evidence or stealing
- Be polite but firm – insist that the owner empties or opens the requested item
- If when searching a person's belongings an item such as a coat or newspaper obscures your full vision or appears to be hiding something, ask the person being searched to move it
- Placing your hands into pockets, bags, or concealed areas not only leaves you open to accusations of dishonesty it also makes you vulnerable to cuts or infection from any sharp objects that may be hidden from view. Always take your own health and safety into consideration when carrying out all aspects of the search.
- When conducting searches, Security Officers should always wear the appropriate protective equipment; e.g. latex or sharp resistant gloves

### ***Five rules of Searching***

1. Ensure you have the person's permission and understanding before you begin the search
2. Ensure your own health and safety at all times
3. Be polite and professional at all times
4. Stick to the search procedures laid down in your assignment instructions
5. Stay in control of the search, be assertive and do not let the person being searched manipulate you

### ***Searching Vehicles***

- Depending on the assignment and level of risk, vehicles may be searched before entering the premises, on leaving the premises, or both. These searches may be random or specific depending on circumstances.
- When searching a vehicle the security officer must be aware of the associated risks and dangers it can entail.

A vehicle should not be searched without the owner present. Permission must be asked and granted before a search of the vehicle can take place. The security officer should utilise the owner as much as possible during the search to avoid accusations of dishonesty against the security officer.

Once the vehicle's owner is present and has given their permission to allow a search to be carried out, the security officer should follow the vehicle search procedures laid down in their assignment instruction. These procedures should contain the following guidelines:

- Before undertaking the search, ensure that the vehicle is parked safely in the designated area



- Ensure that the engine is switched off, the keys are removed from the ignition and the hand brake is on.
- Ensure that there is nobody in the vehicle – the driver and passengers are to remain outside the vehicle throughout the search
- Ensure that the vehicle owner or driver remains with you at all times and is able to witness all your actions
- Ensure that there are no dogs, cats, or dangerous animals in the vehicle
- Ask the owner to open all doors and compartments including the boot and bonnet
- When doors are being opened sand clear in case of falling objects
- Search any concealed areas with a torch and/or probe – never place any part of the hand into concealed areas
- Never touch anything on or in the vehicle – ask the diver to move or open objects
- When searching the engine compartment be aware of hot surfaces
- Whilst carrying out the search be aware of other vehicles and movement
- Ensure you are wearing the correct PPE when carrying out the search
- Be polite and courteous throughout.

#### **4.5 Refusal to be Searched**

Everyone has the legal right to refuse to be searched.

A search cannot be carried out on anyone without their permission and this permission has to be given immediately before the search is carried out.

Agreement before entering the premises or agreement given in a contract of employment does not negate the need to obtain permission each time a search is carried out nor does it count as agreement for every search carried out.

Refusal to be searched does not imply guilt, there may be personal or emotional reasons for the person's refusal. A security officer cannot force a person nor can they threaten to search a person against their will.

Anyone, whether they are an employee, a contractor or visitor, who refuses to be searched on entry to premises should not be allowed entry to those premises. It is the owner's right to refuse admission. A person who refuses to be searched on exiting premises cannot be detained against their will and are at liberty to leave whenever they want.

Detaining people and taking away their liberty to leave constitutes an arrest. If a person is detained by a security officer, simply because they refused to be searched, that person can sue for unlawful arrest.

#### ***If someone refuses to be searched***

If the security officer is confronted by someone refusing to be searched they should adhere to the following guidelines:

- Remain polite and professional
- Ensure that the person understands that they have refused a search
- Politely ask why they have refused to be searched
- Remind them that it is the companies policy that all visitors/personnel are searched
- If not already known ask the person to identify themselves
- Ask them is they will wait to speak to a manager or company representative

- If they refuse to wait, inform them that you will report the incident and let them leave
- Once they have left inform the relevant personnel and complete the necessary paperwork. Any report of a refusal to be search should be accompanied with a full incident report.

Searches may identify stolen or unauthorised items. If the searched person refuses or fails to explain possession and attempts or demands to leave, security officers should consider their safety and follow their assignment instructions at all times.

If it is the company policy to arrest and there is sufficient evidence to justify this course of action, the security officer should again follow the assignment instructions.

When the decision is made, **not** to make an arrest, the person being searched must not be further detained, but every effort must be made to seize the property in question and not allow the person to leave with it if safe to do so.

#### **4.6 Documentation**

Whether the search is specific, random, person, property, or vehicle it must be accompanied by the correct documentation. The style and content of this documentation may differ from assignment to assignment but it needs to be completed and retained every time a search is carried out. An accurate record should prove consistency of professionalism and will help rebuff any false allegations.

Depending on the type of search, the documentation should consist of the following:

- Type of search
- Date and time of search
- Location of search
- Name of security officer carrying out the search
- Name of any witness to the search
- Name of person being searched or vehicle owner
- Vehicle type and registration
- Name of person's company
- Name of person's contact
- Signature of person being searched
- Comments – results of search, details of finds, refusal, etc.

All search documentation should be correlated and filed in a secure location.

#### **4.7 Finding Property During a Search**

The security officer must ask the person being searched to justify why they are in the possession of any property found during a search.

The person being searched may be authorised to be in possession of the property found and the company policy and the assignment instructions will determine what can be accepted as proof of lawful possession.

If no proof can be found nor an acceptable reason can be given then the security officer must act according to their assignment instructions. These instructions will most likely contain the following courses of action:

- Retain the found item – ideally in a sealed evidence bag signed and dated by the person being searched and the security officer
- If the person is a visitor to the site ask them to wait for the relevant contact – manager, escort, etc
- If the person is an employee, they should be allowed to enter the site but their manager should be informed
- Ensure your own health and safety – do not antagonise the person being searched
- If the person refuses to wait do not attempt to forcibly detain them – you may be accused of wrongful arrest
- Until storage of seized items is authorised, ensure that the items are kept in sight of, but out of the control of the searched person
- Complete all of the necessary documentation including an incident report
- Ensure the found property is treated as evidence and secured in a safe place.

## 5 Monitoring Systems

### By the end of this session

The learner will understand the purpose and function of different types of technology, security and monitoring systems in the security environment and will be able to:

- Identify the types and main purposes of security and monitoring technology
- Identify the main features of security, monitoring and emergency systems
- Identify alarm system operator controls and indicators
- List actions to be taken in response to alarm activations
- State the meaning of the term “false alarm”

### 5.1 Types of Security and Monitoring Systems

Many assignments will have different types of security and safety monitoring systems. It is likely to be the security officer's responsibility to set and/or monitor these systems and it is therefore important to have an understanding of the different types.

#### ***Security Systems***

Intruder alarm – These are used to detect the presence of intruders and are activated by different detection devices – e.g. movement detectors, door sensors, fence alarms etc

Access control – These are used to control entry, and exit to and from premises – this not only ensures authorised personnel have access to the site but can also be used for example to provide information for a role call in the event of a fire evacuation.

#### ***Safety Systems***

Fire Alarm (fire and/or smoke) – These are used to detect the presence of fire or the start of a fire i.e. smoke and heat, to alert people or fire control systems to the fact that a fire has started.

#### ***Security and Safety systems***

Closed Circuit Television Cameras (CCTV) – Typically used to monitor and record events at premises or other locations such as shopping centres or entrance and exits to secure sites. They are also used to maintain surveillance on vulnerable people and areas for example the security officer patrolling a fence line

There are different types of camera for different situations: fixed cameras, cameras which will pan, tilt and zoom (PTZ) and dome cameras which may allow 360° coverage.

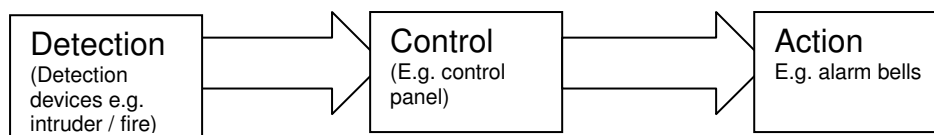
It is the security officer's responsibility on many assignments to set and/or monitor these systems. In some cases this may consist of a small, stand alone system, which has only a very few detection devices.

Other systems may be very large, involving numerous detection devices of different types which are linked to each other, known as '**integrated systems**'

## 5.2 The Functions of Electronic Security Systems

All systems will carry out three functions, which are:

1. Detection – identify a change of state
2. Control – how the change of state is monitored and how the system reacts
3. Action – what the system does in response.



### ***Detection***

#### Intruder alarm

Modern detection devices are very sophisticated and use various types of technology to suit the environment and activity in the area they are required to protect.

They are designed to detect the intrusion of people or objects into buildings enclosed premises or an outside area. Detection is achieved in a number of ways by many differing types of detector – examples of just a few of these include:

- Passive infrared (PIR) detectors; these are widely used space protectors which are activated by changes in temperature e.g. by human body heat, accompanied by movement
- Vibration sensors or break glass detectors on or close to windows/glass panes
- Magnetic door and window contacts, activated by opening/breaking an electrical circuit.

#### Close Circuit Television

CCTV cameras can be programmed in a number of ways. They may be permanently 'on', and are capable of recording all the time, at selected times, or upon command.

They can be, and often are linked to other features of the security system and can for example, be activated by another detection device such as a PIR detector allowing the CCTV system to monitor/record activity in the relevant area.

The main purpose of CCTV systems is to monitor and record events and to maintain surveillance of vulnerable areas or people.

#### Access control

Detection of correct information by keypads/card readers/biometric detection.

Access control systems rely on authorised persons inputting or possessing certain credentials:

- |                              |   |
|------------------------------|---|
| • <b>Something they know</b> | Pin number, password etc  |
| • <b>Something they have</b> | Swipe card/key fobs/proximity card  |
| • <b>Something they are</b>  | Biometrics (unique to them physically, finger prints, palm prints, or iris) |

Examples of detectors used in access control are such things as keypads and card-readers.

- **Keypad** - A number or password is entered into an electronic keypad
- **Card reader** – A card/key fob is either 'swiped' through, or presented to a card reader at the point of entry
- **Biometric Access Control** – An electronic scanner matching details against supplied data from authorised persons e.g. palm or finger prints/eye (iris)

### ***Fire detection equipment***

These detectors are sensitive to heat, flames, smoke and in some instances gas (e.g. carbon monoxide) and when activated the equipment informs the fire control system. They detect the early signs of fire and alert security staff to this.

If a fire is discovered on patrol the security officer can inform the fire control system by using a 'manual call point' (MCP) - either break glass, or push button operation - and so it is essential the security officer is familiar with the location of these manual call points (MCP)

### ***Control***

Control systems communicate with detection devices and alarm devices.

The control function consists of:

- How the electronic security system monitors the information it receives from detectors and
- How it reacts to information it receives from detectors.

### ***Intruder alarm***

Intruder alarms have a control panel which 'decides', from the information received if an alarm condition is warranted. It then instructs the system how to respond.

The person monitoring the system (very often a security officer) is alerted by the control panel receiving a signal which is either displayed on the control panel as an illuminated light or activates a low level audible warning alarm system.

After an 'activation', the control panel will display which areas of the site have been attacked. The assignment instructions or a specific guidance manual will assist in this identification and enable 'response forces' to be directed to attend and investigate the attacked area.

In addition to the low volume audible warning on the control panel, a loud audible warning alarm, usually a siren or a bell, will also activate. This will act as a deterrent, warning would be attackers/intruders that response forces are in attendance and encourage them to leave.

### ***CCTV***

CCTV cameras can be directed automatically by the activation of detectors to provide camera coverage in the affected area. They are usually linked to recording equipment which records permanently or is activated 'on command' by the system.

Where the CCTV is monitored by a control room or central monitoring station the operator is able to view the camera images and respond accordingly.

### ***Access control***

It does what it says! – The system ‘decides’ from the receipt of correct or incorrect information presented by an individual (codes/swipe card etc) whether to allow or deny access.

### ***Fire alarm***

Controlled by the information it receives from the fire detection equipment, including activation of a manual call point (MCP).

## **5.3 What Happens Next?**

After the electronic security system has detected (intruder/fire/access etc) and passed this information to the control, the final stage is what ‘action’ the system takes.

This action is in many different forms dependant on the type of system and may include some or all of the following:

### ***Intruder alarm - Action***

Action at alarm location:

- Audible warnings, internal external sounders – alarm bells, buzzers, sirens, voice broadcast, switching on of floodlights etc

Remote action:

- Automated call to a control room or alarm central monitoring station activating lights/sounds on the display panel to alert the operator.

Recording equipment may be activated which includes:

### ***CCTV - Action***

If they are not permanently monitoring an area cameras may be activated and commanded to cover the relevant area. Additional cameras may be activated e.g. fixed cameras may be switched on if not permanently monitoring, Pan, Tilt and Zoom (PTZ) cameras may be directed to cover the affected zone or to ‘zoom in’ to a specific area. Additional lighting may be switched on to enhance image quality and detail. Recording devices, if not permanently recording images may be activated.

### ***Access control – Action***

The action is very straightforward – The system either allows access or denies access.

### ***Fire detection – Action***

The action by the security system is based on the information provided by the control and will include:

- **Evacuation Sounders** – Sounders (bells/buzzers etc), voice messages – instructing people to leave the building/affected area
- **Lights** - flashing/strobe lights used for example in noisy areas
- **Initiate a call to control room or monitoring centre** to alert the operator
- **Close down ventilation systems**
- **Release of extinguishers**
- **Return of lifts to ground floors** and prevent further use.

### **5.4 Alarm System Operator Controls and Indicators**

Each security and emergency system has a set of controls and indicators. It is vital, if a security officer is to respond correctly, that they know what these controls and indicators are.

#### ***Fire Alarms***

British standards specify that fire systems must indicate by both sight and sound when a fire or an indication of a fire has been detected. They must also indicate by sound and sight when a fault on the system has occurred.

The following controls are compulsory:

#### ***Alarm Indication***

Each Zone **must** have a red indicator which must light up if there is an alarm or activation in that Zone.

A red light will have **one meaning only** – A fire alarm has been activated in that zone and must be responded to accordingly.

In addition the system must have an audible indication that an alarm has been activated and this must be different from the audible alarm indication.

#### ***Fault Indication***

Each Zone **must** have a yellow or amber indicator which must light up if there is an alarm or activation in that Zone.

A yellow light will mean that there has been an occurrence which must be reported and investigated.

In addition, the system must have an audible indication that an alarm has activated and this must be different from the audible alarm indication

**Mute Switches** – Separate switches which silence the alarm or fault indicator.

**Reset Switch** – This switch is the only way a security officer can reset an alarm. The operator should ensure the condition which caused the alarm is no longer present as the alarm will sound again when the reset switch is used.



**Disable/Inhibit switch** - This switch is used to disable part of a system and is normally used to carry out maintenance work. Again there will be an audible and visual indication that part of the system is disabled and these indicators must be different to the alarm and fault indicators.

## **5.5 Actions to Take in Response to Alarm Activations**

A security officer monitoring alarm signals must clearly be able to identify the different sounds and indicator lights made by different types of alarm. With this knowledge a prompt and appropriate response can be initiated to an alarm activation.

### ***Stages of a Response***

#### Initial Response

Response is immediate - this may be an emergency situation. The first thing needed is information and the security officer needs to know where that information can be found.

For example:

- Inspect the control panel to establish the location and nature of the incident
- Assignment instructions will give information about emergency procedures

#### Secondary Response:

Examples include:

- Calling emergency services
- Organisation of evacuation
- Deployment of resources
- Investigation of intruder alarm activation.

Details of the alarm activation should be recorded and if necessary an incident log maintained. A full incident report may also be required.

All alarm activations should be treated as genuine calls until an investigation proves otherwise. Even if an alarm has a history of false activation, any activation should be treated as genuine and responded to accordingly.

## **5.6 False Alarms**

A 'false alarm' is defined as 'an alarm that causes the reaction forces to respond unnecessarily'.

In the security context, of protecting life and property the 'reaction forces' are normally the security officer, the emergency services or owners of the property.

### ***Problems caused by false alarms***

False alarms are a major concern and can cause problems in a number of ways:

- Complacency – numerous false alarms can create complacency within the 'reactionary force' - A 'cry wolf' situation can develop with the danger that if a genuine alarm occurs the response will be poor

- Noise – audible alarms are a warning and deterrent. If however, they regularly activate both these benefits are reduced, and they become a noise nuisance
- Expense – incurred in responding, and also by the interruption to business/loss of production etc
- Police response – police policy is that under certain circumstances, where an alarm has a history of false calls police response to an activation will be withdrawn.

### ***Causes of False Alarms***

There are several causes of false alarms:

- User error – e.g. alarm not correctly set
- Environmental conditions – weather
- Incorrect Installation
- Defective equipment – the system.

## **5.7 Activity**

Without looking back at your notes, try to complete the following activities.

1. List four types of security and monitoring systems you may find on an assignment
2. What is the purpose of an intruder alarm?
3. What is the purpose of an access control system?
4. What is the purpose of CCTV system?
5. What is the purpose of a fire alarm system?
6. What are the three basic functions of an electronic security system?
7. Identify three types of detection system
8. You are in a control room where part of your duty is to monitor the fire alarm panel. An activation on the system occurs – a red light accompanied by a buzzer. What does this tell you?
9. Describe the difference between a fire alarm activation and a fault alarm activation.
10. Name the two stages of response to an alarm activation
11. Where would you find details of emergency procedures?
12. An alarm with a history of false calls activates. Should the security officer monitoring the alarm:
  - A Take no action
  - B Write a fault report for the alarm engineer
  - C Immediately reset the alarm at the panel
  - D Treat as a genuine alarm call
13. Define the term 'false alarm'

14. Which of these is **not** considered a false alarm?

- A Activation caused by adverse weather conditions
- B Activation caused by user not setting alarm correctly
- C Activation caused by faulty detection device
- D Activation caused by alarm equipment being tampered with

15. Which of these is a 'false alarm'?

- A Intruder alarm activated by a burglar
- B Fire alarm activated by smoke
- C Fence alarm activated by a trespasser
- D Activation caused by a faulty detector

## 6 The Law

### By the end of this session

The learner will understand the law and its relevance to the role of a security officer and will be able to:

- Identify relevant legislation
- State the correct procedure to be used when dealing with a trespasser
- Identify arrest procedures
- Identify what is meant by the reasonable use of force
- List the different types of evidence
- State the actions to be taken when preserving evidence
- Identify reporting procedures following a crime

### 6.1 The Importance of Knowing the Law

A security officer will have a good working relationship with the police but that does not mean that security officers are considered to be law enforcement officers or part of the police force.

Security officers are civilians and must abide to and act within the constraints of the law, the same as any private citizen.

Because one of the main duties of a security officer is to ensure the prevention of crime, it is essential that they have a good working knowledge of the law.

A security officer must know:

- The extent of their authority (the same as a normal citizen)
- The difference between 'indictable' and 'summary' offences
- When a crime has been committed
- What type of crime has been committed
- When they can make a citizen's arrest
- How to legally detain someone
- When they can use reasonable force.

### 6.2 Relevant Legislation

#### *Civil Law*

Civil law mostly involves disputes between people, companies or other organisations. If you sue another person or a corporation, or if somebody files a lawsuit against you, your case will end up in County Court in which civil cases are tried.

Civil law offences are not indictable and therefore are not offences for which offenders may be arrested..

## ***Criminal Law***

The most serious matters such as murder, assault, robbery and rape are tried under criminal law. These laws are enforced by the police and the courts, and those breaking them face very serious consequences, including time in prison.

A security officer should have a good understanding of criminal law. Anyone that commits an indictable offence is committing a crime that falls under criminal law and can therefore be arrested by an ordinary citizen

## ***Common Law and Statute Law***

The Common Laws of the United Kingdom have evolved over the centuries. These laws have been progressively developed by judicial decisions. Common Law offences include:

- Murder
- Manslaughter
- Kidnapping.

The statute laws of the United Kingdom are defined and created by Acts of Parliament. These laws sometimes supplant common laws. The following crimes are indictable and therefore the power of citizen's arrest can be used.

## ***Offences Against the Person Act 1861***

Assault: to use force, or threaten to use force against another without their consent.

## ***Theft Act 1968***

Theft: to dishonestly appropriate the property belonging to another with the intention of permanently depriving them of the property.

Robbery: to steal using force, or the threat of force, against a person.

Burglary: to trespass with the intent to steal, inflict grievous bodily harm or cause unlawful damage.

Aggravated Burglary: armed burglary.

## ***Criminal Damage Act 1971***

Criminal Damage: the unlawful intentional destruction or damage of another's property. This includes arson, the destruction of property with fire.

## ***Statute Law - Human Rights Act 1998***

Human Rights Act 1998 gives people the right to take action against the British Government in British courts, with appeal to the European Court of Human Rights should that be necessary. In general, any organisations whose role is of a public nature, or companies undertaking activities on behalf of the state, or any group that spends taxpayers money or has a statutory function or has government appointees on its governing board, are affected by the Act and include local authorities; the Police, schools, universities and colleges; hospitals; and contract companies using CCTV monitoring.

The *rights* of a person under the Human Rights Act are defined by the European Convention on Human Rights. 16 articles of the Convention that have been written into the Human Rights Act. They are:

- The right to life- article 2
- A prohibition on torture – article 3
- A prohibition on slavery and forced labour –article 4
- The right to liberty and security – article 5
- The right to a fair trial – article 6
- No punishment without law – article 7
- The right to respect for private and family life – article 8
- Freedom of thought, conscience and religion – article 9
- Freedom of expression – article 10
- Freedom of assembly and association – article 11
- The right to marry and found a family – article 12
- Prohibition on discrimination – article 14
- Restriction on political activity of aliens – article 16
- Prohibition of abuse of rights – article 17
- Prohibition of restrictions on rights – article 18

Part 2 of these goes on further to protect:

- Property
- The right to education
- The right to hold free elections
- The abolition of the death penalty.

The Human Rights Act defines the scope of an individual's rights in respect of their relation with the State, and in doing so, places limitations on the state in respect of its ability to interfere with those rights. To interfere with these rights, the State must demonstrate that:

- It must be necessary (not just desirable or convenient)
- It must balance public interest against the private rights of the individual (proportionality).

This leads to a situation where some of these rights are absolute, such as the right to life, the prohibition of torture and the right to a fair trial. Other rights are limited or are qualified where they compete with other rights and freedoms.

A security officer could infringe an individual's rights under the Human Rights Act 1998 by, for example:

- Providing false or inaccurate evidence which, if used in court, could stop that individual receiving a fair trial
- Arresting someone without due cause which would be contrary to their right to liberty
- Using CCTV monitoring to record someone in their car would be contrary to the person's right to privacy if it was done without permission of the subject or a warrant to perform 'intrusive surveillance' under the Regulations of Investigatory Powers Act.

Security officers using CCTV in the course of their duties must also ensure that all monitoring is proportional, legal and non-discriminatory.

## **Statute Law - Data Protection Act 1998**

The Data Protection Act 1998 governs the processing of personal data i.e. data about a living person who can be identified from the data. When dealing with people's personal details, it is important to adhere to the following eight principles of the Act, which ensure that personal information must be:

- Fairly and lawfully processed (principle 1)
- Processed for limited purposes (principle 2)
- Adequate, relevant and not excessive (principle 3)
- Accurate and up-to-date (principle 4)
- Not kept for longer than is necessary (principle 5)
- Processed in line with the individual's rights (principle 6)
- Secure (principle 7)
- Not transferred to other countries without adequate protection. (principle 8)

Data includes all information and images captured on CCTV, and the guidance includes acceptable time limits for retaining data. Once a retention period has expired the data must be removed or erased from the records.

CCTV equipment should only monitor what it is supposed to monitor and operators must be aware of the purpose of the scheme and are only allowed to use the equipment for the intended purpose. They must also ensure that all data collected is adequate, relevant and not excessive.

### **6.3 Dealing with a Trespasser**

It is very important that the security officer is aware of the legal constraints and the limit of their powers when dealing with a trespasser. If the security officer does not act correctly it may be them that will be prosecuted for breaking the law.

Despite signs stating that 'Trespassers will be prosecuted', trespass is not a criminal offence but it is an offence under Civil law. Trespassers cannot usually be prosecuted but they can be sued. However, this is very rare due to the expense and inconvenience.

Trespassing is applied to a piece of land open to the public which is not common land, open access land, or a public right of way. Generally land in this country belongs to someone. If you go on to land without the owner's permission, you are trespassing unless there is some right of access for the general public.

Even if the land is owned by a public body, such as the local council, this does not mean necessarily that the general public have a right to be on it at all times.

If the place closes at a certain time and a visitor remains after that time, they can then be considered to be trespassing – the fact that they entered legally earlier that day does not mean that they can remain as long as they wish. Good access and egress control will enable security officers to establish how any trespasser gained entry to the site.

If a visitor contravenes site rules and refuses to leave when asked to do so by a security officer, that visitor becomes a trespasser because they no longer have the landowner's permission to be there even if they entered legally.

The security officer, as the representative of the landowner, can remove an individual from their site. This should only be done under extreme conditions and only with reasonable and

necessary force.

Because reasonable force must be both necessary and justifiable if, as a security officer, you do forcibly eject an individual or an individual's possessions or both you are leaving yourself liable for criminal proceedings for undue force and damage. It is good practice to avoid using force of any kind.

When confronted by a suspected trespasser:

- Ensure your own health and safety only approach the person if you feel it is safe to do so
- Ensure you have an exit route if the person proves to be dangerous
- Inform your control room
- Ascertain the identity of the person and the reason they are there – they may not be a trespasser
- Physically block their path from any direction other than the exit
- Politely ask them to leave
- Inform them that if they do not leave they are trespassing.

If they refuse to leave they are trespassing:

- Continue to tell them that you would rather they left peacefully
- Continue to physically block their path from any direction other than the exit, ensuring that you do not put your own safety at risk by doing so
- Escort them from the premises without using any physical intervention and note which way they go
- Do not use force, unless it is absolutely necessary to do so.

Justification for the use of force may include:

- Their health and safety could be at risk – due to dangers on the site
- Others health and safety could be at risk – depending on the site, its relevant dangers and the actions of the trespasser
- The reasonable belief that the trespasser may cause a criminal offence.

If the situation does not resolve itself the police will have to be called. If the police do attend they can only act as observers. They cannot assist in the removal of the trespassers or their property from the site, but their presence may encourage the trespasser to leave and they can also bear witness to whether any force used could be deemed as necessary and reasonable.

## **6.4 Arrest Procedures**

Security officers are ordinary citizens, they do not have the same powers as the police. However, any person may arrest anyone found committing, or reasonably suspected to be in the act of committing, an indictable offence. For example:

- A person found to be in the possession of stolen property
- A person found in the act of attempting to cause criminal damage by starting a fire
- A person found to be threatening another person with a weapon
- A person discovered climbing into an open window committing burglary



- A person discovered cutting a hole in a security fence line.

To arrest someone means that you are taking away or depriving a person of their freedom and there are serious legal implications to doing this. For this reason, an arrest should only be carried out as a last resort and then only if safe to do so.

The person being arrested must be informed of the following by the security officer making the arrest:

- The name of the arresting security officer – forename and surname
- The fact that arrest is taking place
- The reason for the arrest.

For example “I, Eric Smith, am arresting you for attempted arson”.

After an arrest has been made the security officer has a responsibility for the arrested person’s safety. The arrested person must be observed and monitored continuously until the arrival of the police. This is to ensure that the arrested person does not:

- Attempt to escape
- Inflict self harm
- Pose a risk of injury to anybody
- Dispose of or tamper with evidence
- Contact a confederate.

## **6.5 Reasonable Use of Force**

In England and Wales, anyone can use "reasonable" force when it is necessary to:

- Protect themselves
- Protect others
- Protect property
- Prevent a crime
- Carry out an arrest.

What is considered reasonable force depends on the individuals and the circumstances:

- A heavy weight boxer cannot justify using the same amount of force and ferocity against a professional jockey as the jockey could against the heavy weight boxer
- A five-foot four woman may be able to justify the use of a weapon in defence against an unarmed six foot male assailant, but a six foot male may not be able to justify using a weapon against an unarmed woman.

Reasonable use of force can be used to make a pre-emptive strike on a potential assailant if there is a genuine belief that an attack was imminent and the use of force was absolutely necessary. You do not have to wait to be attacked before you can defend yourself, or another, but you do have to consider stopping or reducing the use of force if and when the ‘need’ to use force no longer exists or the amount of force can be reduced.

This is because the courts may consider that you were unable to make a fully considered judgment at the time and the amount of force used will be considered to have been reasonable if the individual can show that they acted honestly and instinctively.

Reasonable force can also be used if it is necessary to prevent another person from harming themselves.

Any force used will may need to be justified in a court of law. Always remain professional and cool headed and err on the side of caution.

Before resorting to the use of force consider the following:

- Is the use of force necessary?
- Do you have the right to use force?
- What is the minimum amount force needed?
- Can you reduce the amount of force once you have the person under control?
- Can the amount of force you are using be considered reasonable?

## 6.6 Different Types of Evidence

Evidence can be described as 'anything produced before a court which tends to prove or disprove the guilt of a person charged with an offence'. In the same vein that we comply to 'best practices' so we can adopt the same principals to understanding evidence.

### ***The Best Evidence Rule***

The 'best evidence' is 'real' evidence. 'Real' evidence is the 'eye witness' account of events or the actual property that was stolen or the weapon that was used to commit the offence. Other terms that you might hear used to describe 'real' evidence are 'direct' evidence which can sometimes be used in relation to witness statements; and 'primary' evidence which is a term sometimes used to describe items such an actual pieces of stolen property.

'Secondary Evidence' comes in 6 different forms:

- Circumstantial
- Documentary
- Expert
- Opinion
- Corroboration
- Hearsay

<b><i>Circumstantial Evidence</i></b>	Evidence of a series of non-direct facts that can go together to prove the fact.
<b><i>Documentary Evidence</i></b>	Documents, such as 'Incident Books', or 'Search Registers' etc, but includes copies of CCTV footage, 'data' stored on VHS tapes or DVD discs.
<b><i>Expert Evidence</i></b>	This sort of evidence will only be accepted when the court agrees that the person presenting the evidence is indeed an expert. Evidence gathered forensically is recognised as being gathered by experts
<b><i>Evidence of opinion</i></b>	This can only be given by someone who is considered to be an 'expert'.
<b><i>Hearsay</i></b>	Evidence from a third party. It the only type of evidence that is not normally admissible in a court of law. The only exception to this is 'dying declaration'. This is where the third party is

repeating the words said by someone on their deathbed, immediately before they died.

## **6.7 Preservation of Evidence**

### ***The importance of preserving evidence***

The crime scene is a highly important source of physical evidence. A forensic examination of a crime scene is an important part of the investigation which can reveal evidence that can lead to a conviction. It is therefore essential the scene is preserved.

The necessity to preserve evidence by a security officer can arise in a number of ways. It may be by the discovery of a security breach whilst on patrol, or being asked to attend a security breach, the scene of an assault or the discovery of a suspicious package.

Items suspected of being stolen may be discovered during search procedures of people/premises/vehicles etc.

Evidence and scenes of crime need to be preserved to allow police forensic examination and to safeguard the integrity of the evidence.

### ***Action to be carried out at the scene of a crime or incident***

- Remain calm and assess the situation – take notes in your pocketbook of what you see and do
- Advise the control room of the situation
- Ensuring medical assistance to any victim (a priority)
- Unless absolutely necessary don't enter buildings or rooms and restrict others from doing so
- Do not disturb, interfere, touch or destroy anything at the scene and avoid disturbing the approach also. (There may for instance be footprints or blood). However consider ways of protecting evidence from bad weather as this may destroy or contaminate it
- If you're able to identify what has been moved, removed or left behind do so and make notes in your notebook
- Secure the scene and continue to control access until you have been relieved from duty or the police have completed their investigations/examination. Back up your access control by commencing an entry and exit log. Use your pocket book if necessary. This will greatly assist evidence gathering.
- Continuity of evidence/evidence bags/records – evidence e.g. seized from a suspect should be placed in an evidence bag which is then sealed. Date and time should be written on the bag and then signed by the person seizing the item
- Complete notebook.

## **6.8 Reporting Procedures Following a Crime**

If during your work as a security officer you discover or become aware of a crime or incident on your assignment – there is clearly a need for you to report it to someone. But, when do you do this? Who do you report to? And what do you report?

### ***When do you report?***

If the situation involves you making an arrest this must be reported to the police immediately in order that the prisoner can be handed over to their custody with the minimum delay. This is a legal requirement. All details together with any evidence (stolen property/articles used in the commission of the offence etc should be handed over to the police with the prisoner).

Where an arrest is not involved it still may be important that the police are called immediately e.g., the seriousness of the crime, a situation where a forensic examination of the scene is necessary or where the offender(s) may be still in the area.

Incident reports should be completed as soon as practical from pocket book notes (taken at the time) and certainly before you go off duty. All entries in a pocket book and the incident report itself must be signed and dated by the security officer completing the report.

In some instances the police may also ask security officers to complete a witness statement.

### ***Who to report to?***

Could be some or all of the following:

- The Control Room
- Management
- Customer
- Police.

### ***What to report?***

The details of a crime should initially be recorded in the security officer's notebook and should include:

- Date, time, place of incident
- Details of the crime or incident – (theft/burglary/criminal damage etc)
- Details of victims
- Details/descriptions of suspects
- Details of witnesses
- What you did – Report in 'direct speech' any statement made by suspect.
- Details of any evidence recovered (stolen property, weapons, instruments used for breaking and entering)
- Details of who reported to.
- Time of arrival of police etc
- Action you took when the police arrived e.g. handing over evidence etc.

## **6.9 Activity**

Without looking back at your notes, try to complete the following activities.

1. Answer true or false for the following four statements.

- A Murder is covered by Civil Law
- B You can arrest a Trespasser
- C Force should only be used as a last resort and when absolutely necessary
- D A security officer has the same powers of arrest as a police officer

2. Match the crimes listed 1-7 with their explanation listed A-F:

1 Assault

- 2 Theft:
- 3 Robbery
- 4 Burglary
- 5 Aggravated Burglary
- 6 Criminal Damage

- A To trespass with the intent to commit a crime
- B Armed burglary
- C Arson
- D To dishonestly appropriate the property belonging to another
- E To use force, or threaten to use force
- F To steal using force

3. What do you understand by the following terms?

- A Best evidence
- B Circumstantial evidence
- C Hearsay evidence

4. At 7.00am you discover a burglary to an office on the site. It is daylight and there is no sign of an intruder. A ground floor window has been forced open and the frame has been damaged. On the ground underneath the window is a large screw driver. Looking into the office you can see drawers have been opened and you suspect a computer is missing. Office staff are due to arrive for work shortly. Describe what action you would take to preserve the scene for police examination.

5. Why is it important to preserve evidence properly?

- A To ensure continuity of evidence
- B To ensure it is returned to the owner
- C To prevent further offences
- D To ensure it can be disposed of as soon as possible

6. A security officer is conducting a routine search of staff leaving the premises. The member of staff is in possession of property owned by the Company without authority. The property is hidden in a lunch box. Should the security officer:

- 1. Tell the employee involved to hand the item back to the departmental manager when they see them
- 2. Seal the item in an evidence bag, sign, date it and securely store it to preserve its evidential value
- 3. Leave it in the control room for collection by the departmental manager
- 4. Allow the employee to keep it and later report it to your supervisor

7. Why is it important that the police are informed straight away when someone is arrested?

8. What item should a security officer carry and use for initially recording details of crime or other incidents?

- A Incident report

- B Blank Paper
- C Daily occurrence log
- D Notebook

9. An incident report is completed by a security officer to:

- A Record details of patrol activity on a daily basis
- B Ensure colleagues know what is happening on the site
- C Accurately report details of a crime or incident
- D Demonstrate to the supervisor the job is being done correctly

## 7 The Importance of Reporting and Record Keeping

### By the end of this session

The learner will understand the importance and purpose of reporting and record keeping and will be able to:

- List the different types of records relevant to the role of a security officer
- Identify the do's and don'ts of report writing
- State the importance of an incident report
- Identify the information to be recorded in an incident report
- Identify the do's and don'ts of keeping a notebook
- Identify the content and importance of a hand-over
- Use the NATO phonetic alphabet

### 7.1 The Different Types of Records Relevant to a Security Officer

Security officers are required to complete various different reports and registers on a site. They may be handwritten or in some cases, computer based, and will include all or some of the following:

- **Assignment Instructions** - a reference manual containing information which is needed for security officers to carry out their duties effectively. They form part of the contract between the Customer and the Security Company, showing the customer's requirements
- **Accident Book** – Used to record details of any accidents on site
- **Daily Occurrence Book** (Site Log Book) – Used to record brief details of occurrences/activity on site
- **Duty Sheets** – Security officers' duty rotas
- **Handover Records** – Records to show handover procedures have been carried out correctly
- **Incident Reports** – Comprehensive reports of incidents/unusual occurrences
- **Key Register** - Used control access to keys by signing them in and out
- **Patrol Log** – Details all patrol timings
- **Pocket Books** – Carried by security officers to make routine entries and contemporaneous notes of any incident etc
- **Search Register** – Register of vehicles/people searched
- **Visitors Book** – Register of visitors entering and leaving site
- **Written Evidence** – Statements.

### 7.2 The Do's and Don'ts of Report Writing

Routine activities which are a daily or regular occurrence, such as shift handovers, issue and receipt of keys, arrival and departure of staff, visitors etc are normally recorded in the appropriate book/register specific to that purpose.

Where a situation of a serious or unusual nature occurs a detailed and accurate report will be required. For this an incident report will be completed.

### **DO:**

- Only use black pen
- Ensure your report is legible and understandable
- Use clear, simple English and, if necessary, print them out
- Plan what to say before starting
- Record the information as soon as practicable
- Sign and date all entries
- Correct all errors by crossing out using a single line and initial the alteration

### **DO NOT:**

- Use jargon or abbreviations
- Use pencil as it smudges and can be altered
- Use correcting fluids
- Tear or remove pages from book or register etc

Remember that reports can include diagrams as well as words if this helps to describe a situation.

### **Key considerations**

When writing a report, remember that in the future you may be questioned on its content, It could for instance become evidence in court. It is wise to take a few moments to plan the content of the report and how you will structure it. This will help to ensure you include all relevant detail in such a way that is easy for the reader to understand.

A 'well tried' guide to the structure and content of a report which will ensure incidents or situations are recorded correctly is to address the following within the report.

The six points to cover are:

- 1 WHO?.....was involved
- 2 WHAT?... ..happened
- 3 WHERE?... did it happen
- 4 WHEN?.....did it happen
- 5 WHY?.....did it happen
- 6 HOW?.....did it happen

## **7.3 The Importance of an Incident Report**

The nature of a security officer's work is likely to lead to the records, of situations and incidents they become involved with, being required in the future.

An incident report is a detailed report required for a non-routine activity and might for example be needed for:

- Internal auditing
- Insurers
- Trade Unions
- Health and Safety records



- The Police – where any criminal activity is involved and evidence is required for use in court
- To provide continuity of evidence where images have been captured on CCTV.

They may not be needed for months after they have been written, when recollections of the event may start to fade.

A properly written incident report, written as soon as possible after the event, is therefore essential while events are still fresh in the mind. Its importance can be summarised as follows:

- As a permanent record of an incident – it can protect a security officer, and the organisation, from suggestions that their recollection of events is inaccurate or that duties weren't carried out correctly
- Others can use it to assist in deciding a course of action – it may be used as evidence in court proceedings or health and safety enquiries
- It is an efficient way of consolidating facts taken from different sources – this enables auditing and provides a way of monitoring information.

#### **7.4 The Information to be Recorded in an Incident Report**

As already discussed your assignment instructions will dictate that an incident report will invariably be needed when an unusual or serious situation occurs. Some examples of these situations requiring a report are:

- Crime – criminal damage/theft/burglary
- Suspicious incident or situation
- Incidents involving members of the public e.g. trespassing on site
- An accident causing injury or damage
- Evacuation of premises for any reason
- Breach of or non-compliance with health and safety requirements.

This list is not exhaustive and incident reports may be required for other events.

Incident reports should be factual. Opinions should not generally be included in the report and if they are it should be made very clear that it is an opinion only.

#### ***The Report***

The content of your report should contain the following:

##### Beginning

- Identify yourself
- The date and time of the report
- Identify the reports recipient(s).

##### Middle

- Date and time of the event
- Details of persons involved by name and/or description - did you know them?
- Names of any witnesses
- Where - The exact place where the event took place

- Complete details of what happened - this will include some or all of:
  - What you were doing at the time?
  - What did you do?
  - What did you see?
  - What did you say? - exact words
  - What did other people do?
  - What did other people say?- exact words
  - What was the weather like – if relevant, it may be a factor e.g. visibility
  - What happened then?
  - Who did you tell? – colleague/supervisor/emergency services?
  - When did they arrive? – if they attended!
  - Why did it happen? – if you're able to say
  - How did the incident occur? – if you're able to say
- Details of any force used and reasons why the force was necessary.

End

- Date and signature of person making the report.

Utilise pocket book entries made at the time of the event to assist in writing your report.

## **7.5 Use of Pocket Notebooks**

A security officer's notebook is an essential and important piece of equipment which should be carried at all times when on duty. It will contain confidential information and should be kept in a safe, secure place when not on duty. It is the document used to record your daily, routine activities and for recording full details of an incident or unusual event. These original notes should be made at the time of, or if not practical to do so, as soon as possible after an event.

There are rules which need to be followed when using your notebook.

### ***DO:***

- Carry your notebook at all times when on duty
- Use your notebook to record routine and unusual events
- Make detailed notes at the time, or, if not practical to do so, as soon as possible after the event whilst still fresh in your memory
- If someone says something, write it down in their words
- Make entries in black ink or ballpoint pen
- If a page is left blank in error draw a diagonal line straight across the page and initial
- If a correction is needed draw a single line through the word(s). Ensure it remains legible, and initial the alteration
- Write on every line or draw a line through any part of a line not used and initial (to prevent any additions, or allegations that additions have been made at a later date)
- Sign and date every entry in the book so that an entry can be used as evidence.

### **DO NOT:**

- Use the notebook for any personal reason – remember it could be required in court in the future
- Tear out any pages
- Erase any words
- Overwrite or obliterate words making the original entry illegible
- Leave blank spaces
- Write between lines – this can indicate notes inserted afterwards.

A main reason for these rules is to ensure there can be no allegation or suspicion that an entry has been changed or added to.

## **7.6 The Content and Importance of a Hand-Over**

At shift hand-over it is important, that all necessary information, documentation, and equipment are passed on to the incoming shift. This will ensure that security officers are properly briefed and equipped to maintain security.

### ***Hand-Over Procedures***

- Allow sufficient time when reporting for duty to carry out a thorough handover
- Incoming officer should read back through the daily occurrence book/incident report book to the last time they were on duty to be aware of any incidents, suspicious situations etc
- Equipment – Discuss any deficiencies in equipment e.g. faulty radios, faulty alarms etc. Are there any outstanding keys? On-going deficiencies must be reported continually until repaired or no longer in action.
- Discuss ongoing incidents, identifying any outstanding actions that are needed
- Ensure all messages received during the shift have been dealt with, or passed on to be 'actioned'
- Documentation – All relevant documentation should be completed before going off duty
- Finally, check all relevant keys and all other equipment are in the control of the incoming shift and not for instance left inadvertently in the pocket of an officer going off duty.

## **7.7 The NATO Phonetic Alphabet**

The NATO (North Atlantic Treaty Organisation) phonetic alphabet was developed to assist in verbal communication being clearly understood, to ensure the message sent was the message received. This also reduces the necessity for messages to be repeated and keeps the air waves clear.

Messages should be:

A - Accurate

B - Brief

C - Clear

The alphabet uses an agreed word for each letter and if the sender and receiver are familiar with the alphabet, the chance of the listener confusing letters and getting the message wrong is vastly reduced.

We've all no doubt had to ask someone to repeat a spelling at some time or other. The letters P, B & D for instance can sound very similar, particularly if not spoken clearly or if they are passed by radio or telephone when reception is poor.

Using the phonetic alphabet these letters would be pronounced 'P – Papa, B- Bravo, D- Delta'. They now each sound very different and can easily be distinguished from each other. The phonetic alphabet should be used in radio and telephone communications where necessary e.g. to spell names, give car registration numbers etc.

### ***The Phonetic Alphabet***

<b>Alpha</b>	<b>Foxtrot</b>	<b>Kilo</b>	<b>Papa</b>	<b>Uniform</b>	<b>Zulu</b>
<b>Bravo</b>	<b>Golf</b>	<b>Lima</b>	<b>Quebec</b>	<b>Victor</b>	
<b>Charlie</b>	<b>Hotel</b>	<b>Mike</b>	<b>Romeo</b>	<b>Whiskey</b>	
<b>Delta</b>	<b>India</b>	<b>November</b>	<b>Sierra</b>	<b>Yankee</b>	
<b>Echo</b>	<b>Juliet</b>	<b>Oscar</b>	<b>Tango</b>	<b>X-ray</b>	

An operator using the phonetic alphabet to spell the word 'security', as an example would say 'Sierra, Echo, Charlie, Uniform, Romeo, India, Tango, Yankee'

Similarly, to eliminate confusion there is also a recognised method for transmitting numbers. There are variations to this, but, in general, all numbers are communicated singularly; for example, to transmit the number 66 we would not say "sixty six", but would say each letter separately; "Six, six".

Therefore all numbers are an amalgamation of just the figures 0 to 9 and are pronounced more effectively using the following terminology:

0 = Zero  
1 = Wun  
2 = Too  
3 = Thuree  
4 = Fower  
5 = Fife  
6 = Six  
7 = Seffern  
8 = Ate  
9 = Niner

In practice, it may aid transmission and understanding to use a combination of the two ways; so, in the example above, to transmit the number 66 you would say, "Six, Six. I say again. Sixty Six."

Or a car registration Number e.g. AB 55 CEF becomes 'Alpha, Bravo, Fife, Fife, Charlie, Echo, Foxtrot.'

## 7.8 Activity

Without looking back at your notes, try to complete the following activities.

1. Identify eight different types of records relevant to the work of a security officer
2. List four do's of report writing

DO.....  
DO.....  
DO.....  
DO.....

3. List four don'ts of report writing

DO NOT.....  
DO NOT.....  
DO NOT.....  
DO NOT.....

4. Describe briefly the three parts of a report and their content
5. Describe the three main reasons why an incident report is important
6. Give five examples of situations when an incident report will be required
7. Describe six points to cover when writing an incident report?
8. Which of these should be included in the beginning of an incident report?
  - A Description of suspects
  - B Weather conditions at the time
  - C Name of the person making the report
  - D What the person said
  - E Time of arrival of emergency services
  - F Date of report
  - G Name of recipients of report
9. You are making an entry in your notebook and discover you have left a page blank – What should you do?
  - A Tear it out
  - B Cross the entire entry out and start again
  - C Get a new notebook and start again
  - D Draw a diagonal line across the blank page and initial it.
10. What is the main reason for notebook entries being completed at the time of, or if not practical to do so, as soon as possible after an event?
  - A So the supervisor can check it
  - B Because the details are still fresh in the memory

- C Because the assignment instructions require it
- D Because the Police might need it

11. What **must** a security officer do if they make an error in a pocket book entry?

- A Use correcting fluid and write over it
- B Obliterate the incorrect word(s) and write the correction above it
- C Draw a line through the incorrect word(s) so it remains legible and initial the correction
- D Cross out the entire page and start a new one

12. Why is it important that a thorough handover takes place between the outgoing and incoming shift?

13. You are coming on duty. Please describe how you would ensure you are properly briefed and equipped for your duties.

14. You are going off duty – How do you ensure the incoming shift are properly briefed and equipped for their duties?

15. Use the phonetic alphabet for each letter in the following sentence

‘The quick brown fox jumped over the lazy dog’

16. Write the following registration numbers as if you were passing them over the radio to another security officer using the phonetic alphabet

- NU 59 CAR
- MT 01 BDG
- S 332 VWJ

## 8 Activity Answers

### The role of a security officer within the private security industry activity answers

1. To deter and protect
2. Protection of life  
Protection of property and premises  
Prevention of loss and waste  
Prevention and detection of crime
3. Waste  
Breach of confidentiality
4. Robbery  
Burglary (break-ins)  
Criminal damage including graffiti  
Theft  
Deception  
Assault  
Breach of the peace  
Public Order Offences  
Trespass
5. Details of overtime rates  
Holiday entitlement for security staff  
Security officer's personal details  
Training records  
Grievance procedures
6. a) In the assignment instructions
7. b) Overtime rates
8. c) To act as a reference manual for security officers which contains information essential to their duties.
9.
  - High visibility clothing
  - Protective footwear
  - Hard hats
  - Goggles
  - Gloves
  - Ear defenders
  - Wet weather clothing

- 10.
- Torch
  - Clocking device
  - Swipe card
  - Radio/phone
  - Pocket book/pen
  - Pager
- 11.
- Employee information
  - Client information
  - Sensitive company documents
  - Security procedures
  - Location of detection equipment
  - Alarm codes
12. d) Do not give the information as it is confidential. Try to identify the caller and inform your supervisor.
13. d) Don't give any information and advise your supervisor
- 14.
- Provides emergency support and back up
  - Assists with enquiries
  - Monitor the security officers' safety with check calls
  - Plans the site coverage by co-ordination of security officers activities
  - Monitors Radio and other communications
  - Monitors CCTV and alarm systems
15. A False  
B True  
C True  
D True  
E False

### **Patrolling activity answers**

1. The initial patrol i.e. first patrol of the shift  
The subsequent or interim patrol  
The specific patrol  
The final/last patrol
2. If the initial patrol coincides with the site closing down at the end of their business day, then this patrol is known as a 'Shut down' patrol and this is when the site need to be secured. However, if the final patrol is when the site closes then this is when a security officer will need to ensure that all is safe and secure.
3. Inform the control room  
Ensure that their equipment is working  
Ascertain if there any areas of concern  
Check that all your equipment is in working order  
Make a radio check call  
Log the start time of the patrol  
Ensure that all unnecessary electrical appliances are switched off



Ensure that any other health and safety instructions are complied with  
Secure the security base area

4. Preserve their health and safety  
Preserve the health and safety of others  
Preserve the integrity of the site  
Prevent loss or damage
5. Is there smoke, or flames, coming from the building?  
Are there any signs of forced entry?  
Are there any unusual lights, shadows, or noises?
6. Record all of your findings in your pocket notebook
7. Torch  
Radio  
Keys and/or access card  
Pocket notebook and pen  
PPE (personal protective equipment)  
Landline telephone  
Clocking
8. Local knowledge  
Site knowledge
9. Inform the control room and any other relevant persons  
Secure the area  
Preserve the evidence  
Ensure that the security of the site is re-established as soon as it is practicable to do so

### **Monitoring systems activity answers**

1. Intruder alarm, access control, CCTV, fire alarm
2. An intruder alarm
3. An access control system control entry and exit, to and from a premises
4. CCTV is used to monitor and record events at premises, and to maintain surveillance on vulnerable people and areas.
5. A fire alarm system detects the presence of fire or the start of a fire
6. Detection, control, action
7. Intruder alarm, CCTV, access control, fire detection equipment
8. A fire alarm has activated
9. Fire alarm indication
  - Each Zone must have a red indicator which must light up if there is an alarm or activation in that Zone
  - In addition the system must have an audible indication that an alarm has activated

### **Fault Alarm Indication**

- Each Zone **must** have a yellow indicator which must light up if there is an alarm or activation in that Zone

- The system must have an audible indication that an alarm has activated and this must be different from the audible alarm indication
10. Initial, Secondary
  11. In the Assignment Instructions
  12. d) Treat as a genuine alarm call
  13. 'An alarm that causes the reaction forces to respond unnecessarily'
  14. d) Activation caused by alarm equipment being tampered with
  15. d) Activation caused by a faulty detector

### **The law activity answers**

1. True or False
  - E False - Murder is covered by Criminal Law
  - F False - Trespasser is not an indictable
  - G True – Force should only be used as a last resort and when necessary. The level of force used must be reasonable and you will need to justify the use of any force
  - H False - A security officer has the same powers of arrest as a any normal citizen, not police officer
  
2. Match the crime:
  - 1-E
  - 2-D
  - 3-F
  - 4-A
  - 5-B
  - 6-C
  
3.
  - A Real evidence such as an 'eye witness' account of events or the actual property that was stolen or the weapon that was used to commit the offence
  - B Evidence of a series of non-direct facts that can go together to prove the fact.
  - C Evidence from a third party. It the only type of evidence that is not normally admissible in a court of law. The only exception to this is 'dying declaration'. This is where the third party is repeating the words said by someone on their deathbed, immediately before they died.
  
4.
  - Remain calm and assess the situation – take notes in your pocketbook of what you see and do
  - Advise the control room of the situation
  - Unless absolutely necessary don't enter buildings or rooms and restrict others from doing so

- Do not disturb, interfere, touch or destroy anything at the scene and avoid disturbing the approach also. (There may for instance be footprints or drops of blood) However consider ways of protecting evidence if for instance bad weather may destroy or contaminate it
  - If you're able to identify what has been moved, removed or left behind do so and make notes in your notebook
  - Secure the scene and continue to control access until the police have completed their investigations/examination
  - Continuity of evidence/evidence bags/records – evidence e.g. seized from a suspect should be placed in an evidence bag which is then sealed. Date and time should be written on the bag and then signed by the person seizing the item
  - Complete notebook.
5. A) To ensure continuity of evidence
  6. B) Seal the item in an evidence bag, sign, date it and securely store it to preserve its evidential value
  7. When an arrest is made the prisoner must be handed over to the Custody of the Police with the minimum delay
  8. D) Notebook
  9. C) Accurately report details of a crime or incident

### Report writing activity answers

1.
  - Accident book
  - Daily occurrence book
  - Duty sheets
  - Handover records
  - Incident
  - Key register
  - Pocket books
  - Search register
  - Visitors book
  - Written evidence
2. Any four of the following:
  - DO** Only use black pen
  - DO** Ensure your report is legible and understandable
  - DO** Use clear, simple English and, if necessary, print them out
  - DO** Plan what to say before starting
  - DO** Record the information as soon as practicable
  - DO** Sign and date all entries
  - DO** Correct all errors by crossing out using a single line and initial the alteration
3.
  - DO NOT** Use jargon or abbreviations
  - DO NOT** Use pencil as it smudges
  - DO NOT** Use correcting fluids:
  - DO NOT** Tear or remove pages from book or register etc.

4. A beginning – Including the subject of the report, who the report is from (author), who the report is to (recipient(s)) and include the date.

A middle – This is the main body of the report containing detailed information

An end – At the end of the report the author should show who wrote the report and when by signing and dating the document sign their name and date

5.
  - As a permanent record of an incident
  - Others can use it to assist in deciding a course of action
  - It is an efficient way of consolidating facts taken from different sources

6.
  - Crime – criminal damage/theft/criminal damage
  - Suspicious incident or situation
  - Incidents involving members of the public e.g. trespassing on site
  - An accident causing injury or damage
  - Evacuation of premises following fire alarm
  - Evacuation of premises following or suspecting gas or chemical leak
  - Breach of or non-compliance with health and safety requirements

7.
  - WHO? was involved
  - WHAT happened
  - WHERE? did it happen
  - WHEN? did it happen
  - WHY? did it happen
  - HOW? did it happen

8. C, F, G

9. d) Draw a diagonal line across the blank page and initial it.

10. b) Because the details are still fresh in the memory

11. c) Draw a line through the incorrect word(s) so it remains legible and initial the correction.

12. To ensure that security officers are properly briefed and equipped to maintain security.

## Learning Outcomes and Assessment Criteria

### Working as a Security Officer

Learning outcomes	Assessment criteria
The Learner can:	The Learner will:
1. Understand the role of a security officer within the private security industry	1.1. Identify the main responsibilities of a security officer 1.2. Identify the purposes of assignment instructions 1.3. List items of equipment needed when on duty 1.4. Explain the term “confidentiality” within the context of a security officer’s responsibilities 1.5. Identify the purposes of control rooms
2. Understand the importance of, and reasons for, patrolling	2.1. Identify the types and purposes of different patrols 2.2. Identify actions that should be taken before starting a patrol 2.3. Describe patrolling procedures and techniques 2.4. State the equipment required for patrolling 2.5. Explain the importance of vigilance and using local and site knowledge when patrolling
3. Understand how to control access to and egress from a site	3.1. Identify the purposes of access and egress control 3.2. Identify duties of a security officer when using different methods of access and egress control 3.3. State the powers and identification requirements of statutory agencies
4. Understand basic search procedures	4.1. List the conditions that have to be in place before searching can be carried out 4.2. Identify the different types of search 4.3. State the correct procedures for carrying out personal and vehicle searches 4.4. State actions to be taken in the event of a refusal to be searched 4.5. State the information to be recorded in search documentation 4.6. State the action to be taken when property is found during a search

Learning outcomes	Assessment criteria
The Learner can:	The Learner will:
<p>5. Understand the purpose and function of different types of technology, security and monitoring systems in the security environment</p>	<p>5.1. Identify the types and main purposes of security and monitoring technology            5.2. Identify the main features of security, monitoring and emergency systems            5.3. Identify alarm system operator controls and indicators            5.4. List actions to be taken in response to alarm activations            5.5. State the meaning of the term “false alarm”</p>
<p>6. Understand the law and its relevance to the role of a security officer</p>	<p>6.1. Identify relevant legislation            6.2. State the correct procedure to be used when dealing with a trespasser            6.3. Identify arrest procedures            6.4. Identify what is meant by the reasonable use of force            6.5. List the different types of evidence            6.6. State the actions to be taken when preserving evidence            6.7. Identify reporting procedures following a crime</p>
<p>7. Understand the importance and purpose of reporting and record keeping</p>	<p>7.1. List the different types of records relevant to the role of a security officer            7.2. Identify the do's and don'ts of report writing            7.3. State the importance of an incident report            7.4. Identify the information to be recorded in an incident report            7.5. Identify the do's and don'ts of keeping a notebook            7.6. Identify the content and importance of a hand-over            7.7. Use the NATO phonetic alphabet</p>