UNITED ARAB EMIRATES
MINISTRY OF INTERIOR
GEN. DIRECTORATE FOR SECURITY SUPPORT

الإمارات العربية المتحدة
وزارة الداخلية
الإدارة العامة للإسناد الأمني

إدارة تنظيم شركات الأمن الخاصة
PRIVATE SECURITY FIRMS REGULATORY DEPT.

Security Operation – Level3

Private Security Firms
Regulatory Department

ADVETI

VEDC
Vocational Education
Development Centre
مركز التعليم والتطوير المهني

إدارة تنظيم شركات
الأمن الخاصة

Table of content:

Module 1
First Aid

Module 1

First Aid

Qualification Link

Units

- HLT03015NU17-Apply Basic First Aid Skills

Learning outcomes

1. Conduct an Initial incident scene assessment
2. Provide Primary Care
3. Report incident and care provided

1.1. Aims and principles of first aid

First aid is the immediate care given to a casualty until qualified medical personnel can take over. The aim of first aid can be remembered by 3 Principles:

- Preserve life
- Prevent further harm
- Promote recovery

This is commonly referred to as the 3 P's of first aid.

Key information

Basic Life Support

This is a term given to the provision of the following 3 elements:

- Initial assessment of a casualty
- Maintaining an airway and breathing
- Resuscitation – CPR

Catastrophic Bleeding

If a casualty is bleeding from a major artery, death will occur within a matter of minutes. If there is obvious heavy bleeding, treat this as first priority before continuing with the cycle of primary care

1.2. Responsibilities of a first aider

As a trained first aider your responsibilities will include:

- Assessing a medical emergency quickly and safely, calling for appropriate assistance
- Identify the injury or illness
- Give early and appropriate treatment in order of priority
- Comfort and reassure a casualty
- Hand over to emergency services
- Prepare and submit incident reports

Figure 1 - First Aid Responders

1.3. Scene assessment

Topic focus

First responder actions

- Look for danger
- Control hazards to self and others
- Send for help

When arriving at the scene of an injury or medical incident it is important to quickly survey the area and establish the following:

- What physical hazards are present?
- How can risk of further harm be reduced?
- Levels of consciousness of the casualty or casualties
- Send for help

Key to the welfare of all involved, is controlling hazards present at an incident site. Types of hazards could include:

- Vehicles and traffic
- Machinery and equipment
- Live electricity
- Contaminants or chemicals
- Debris and damaged construction materials
- Flammable liquids or gases

Figure 2 - Common hazards

Assessing the consciousness of a casualty will guide decision making for further treatments. The method used to determine the level of consciousness of a casualty is known as AVPU:

- **Alert** – is the casualty moving or talking? If no, proceed to V
- **Voice** – Does the casualty respond to your voice? If no, proceed to P
- **Pain** – Does the casualty respond to minor pain caused by you? E.g. flick the eyeball, Rub the sternum with knuckles. If no, proceed to U
- **Unresponsive** – Assume that the casualty is unconscious and unresponsive

Sending for help is critical in order to activate the emergency services response. For serious injury, the time taken for qualified medical staff to attend the scene may be a significant factor in the survivability of the casualty.

Remember:

- Shout and send for help
- Dial 999 if possible
- Do not leave a casualty that is not breathing, or has suffered cardiac arrest

1.4. Primary care

Primary care is the term given to the set of actions taken by a first aider to provide basic life support - **BLS**.

Danger and Response are checked during the scene assessment. ABCD belong in the phase of primary care.

A – Airway. Inspect the airway of the casualty for obstructions:

- Position the casualty on their back
- Gently tilt the head back, and lift the chin
- Look for any obstruction
- Clear obstructions with a sweeping motion ensuring that the object is not forced further into the airway

Figure 3 - Head tilt

B – Breathing. Look listen and feel for normal breathing:

- Place your ear next to the casualties' mouth to listen
- Look down to the chest to see the rise and fall during breathing
- Place a hand on the chest to feel the chest move during breathing
- Take no longer than 10 seconds to perform this step

C – Circulation. If the casualty is not breathing, and showing no sign of life:

- Begin CPR
- If possible, send somebody to get an AED
- Provide 30 Chest compressions and 2 Rescue breaths
- Continue this cycle until help arrives
- If an AED arrives switch to using it

CPR for babies

If a baby requires CPR, use the following method:

- Tilt the head back to open the airway
- Make a seal with your mouth over the babies nose and mouth
- Blow for 1 second, the chest should visibly rise
- Give 30 compressions, with 2 fingers to the centre of the baby's chest

- The compression should go to 1/3rd of the depth of the baby's chest

Safety!

- If it is available, use a shield to prevent transmission of infection during rescue breathing

1.5. Defibrillation (AED)

Figure 4 - Automated External Defibrillator

If a casualty has suffered cardiac arrest, the use of an AED can significantly increase the chance of survival. An AED will provide electrical stimulation to the heart, and attempt to trigger a normal rhythm. An AED is very simple to use, and once turned on you will be prompted to follow instructions that normally include:

- Exposing the casualties' bare chest
- Placing adhesive pads onto the chest
- The AED will analyse the casualties heart rhythm
- If the AED determines that a shock is required, it will automatically charge up and tell you when to press the button to deliver the shock
- Once the shock has been delivered, the AED will prompt you to check for normal breathing and heartbeat. If not, you will be reminded to resume CPR

Safety!

- Do not touch the casualty while the AED is analysing the heartbeat – this will interfere with electrical signals
- Be aware of water when using the AED, for example at a pool or in a bathroom – This presents a electrocution hazard

1.6. The recovery position

The recovery position is used to keep an unconscious casualties' airway open, and allow normal breathing

1.6.1. Recovery position for adults

The following steps can be followed to place an adult into the recover position:

- Kneel next to the casualty
- Place the arm nearest to you across the casualties' body, with the palm facing upwards
- Take their other arm and bring it across the chest so that the back side of their hand is touching the cheek nearest to you
- Hold that hand in position, and with your other hand, lift the far side knee up until their foot is flat on the floor
- Roll them onto the side, pulling the bent leg towards you

Safety!

- If you think that the casualty has a spinal injury, you must not move them. Instead, gently open the jaw to provide an airway and seek immediate medical assistance.

1.6.2. Recovery position for a baby

If a baby is breathing normally, but is unresponsive, cradle them in your arms with the head tilted downwards. This will allow the airway to remain open, and prevent choking. Immediately call for medical assistance.

1.7. Treating shock

Shock is a serious condition that occurs when there is not enough blood flow throughout the body. This means that vital organs can become deprived of oxygen and damage can occur to the brain or heart.

Shock can be caused by a variety of factors including:

- Heart failure

- Severe bleeding (internal or external)
- Dehydration, vomiting, burns, diarrhoea
- Severe infection or allergic reactions

Symptoms that could indicate a casualty is experiencing shock include:

- Pale face
- Cold, clammy skin
- Fast and shallow breath
- Fast and weak pulse
- Yawning and sighing
- Confusion

To treat a casualty for shock:

- Lay them down, with head low and legs raised up
- Loosen any tight or restrictive clothing
- Cover them with a blanket or jacket
- Monitor breathing, pulse and conciousnous until medical assistance arrives

1.8. Wound and condition treatment

1.8.1. Catastrophic bleeding

If a casualty has catastrophic bleeding, this must be treated as a priority.

Bleeding from the head, neck or torso:

- If there is any object stuck in the wound, leave it in place
- Remove any clothing from the wound site
- Apply a heavy bandage directly to the wound
- Use firm direct pressure into the wound
- If bleeding is not controlled, continue to add fresh bandages and pressure to the wound site
- Secure bandages in place, and observe the wound for resumed bleeding
- Treat the casualty for shock
- Support the injured area

Bleeding from a limb:

- Apply a tourniquet to the limb as low as possible next to the wound site
- Apply bandages to the wound site with firm direct pressure
- Secure bandages in place, and observe the wound for resumed bleeding
- Treat the casualty for shock
- Support the injured area

1.8.2. Minor cuts and grazes

- Clean the wound under water, or use sterile wipes
- Pat the wound dry using a clean cloth
- Cover the wound with a gauze dressing, and raise it to help stop the bleeding
- Remove the gauze, and apply a clean dressing to the wound

1.8.3. Spinal injury

The most common cause of a spinal injury is extreme force, twisting or bending. Possible causes of a spinal injury can include:

- Falling from height
- Diving into a shallow pool
- Involved in a vehicle accident
- Hit by a heavy object to the back
- Hit in the head or face

Symptoms may include:

- Pain in the neck or back
- Twisted or abnormal shape of the spine
- Bruising of the skin over the spine

Treatment for suspected spinal injuries:

- Stop the casualty from moving
- Immobilise the head and neck – Kneel behind the head, rest your elbows on the ground and support the head in alignment with the neck and spine
- Reassure the casualty, and await medical assistance

1.8.4. Bleeding nose

Key information

- If a casualty has been hit on the head and blood from the nose is thin and water, this may indicate a skull fracture. This is very serious and emergency medical help should be called immediately.

When treating a bleeding nose, the priority should be to control the bleeding and keep the casualties' airway from becoming obstructed. Take the following steps to treat a bleeding nose:

- Sit the casualty down, and have them lean forwards – this will ensure blood doesn't run down their throat, blocking the airway
- Tell the casualty to breathe through their mouth, and pinch their nose until the bleeding stops

- Tell the casualty not to speak, cough or sniff as this may cause clotted blood to break and start bleeding again

1.8.5. Choking

Key information

- A choking casualty that makes **NO** noise, is in serious trouble.

If you see somebody that you think is choking, ask them. If they can speak to you, they should be able to clear their own throat by coughing. If they can't cough or make any noise, they will need immediate help. Ask someone else to call for help and then:

- Lean the casualty forward
- Use the heel of your hand to give 5 sharp slaps between their shoulder blades
- Check inside the mouth for any loosened object, and ask them to remove it.

If this doesn't clear the blockage,

- Stand behind the casualty
- Link your hands just below the bottom of their chest
- With your lower hand clenched in a fist, pull quickly inwards and upwards

Continue to cycle through slapping the back and thrusting the abdomen until the blockages is cleared. If the casualty becomes unconscious, check the airway and begin CPR.

1.9. Casualty management and reporting

Having provided primary care, treatment of wounds and reassurance of a casualty, there is an opportunity to conduct a secondary survey of the casualty, and further management of the scene. It is good practice to keep notes, as this will enable you to complete an informative hand over of the casualty to medical professionals, and support the preparation of an incident report.

The secondary survey will include:

- Asking the casualty exactly what happened
- Ask witnesses to describe the incident
- Ask the casualty about their medical history:
    - Allergies
    - Medication
    - Previous conditions
    - Last meal
    - Event history – what just happened
- Head to toe examination – checking for further injuries or symptoms

Topic focus

Casualty management & reporting

- Keep basic notes
- Continue to monitor casualty symptoms and condition
- Highlight any hazards present to incoming medical staff

Be prepared to give a short summary of this information to the medical team that arrives at the scene.

An incident report will also be required by your organisation in order to comply with documentation and reporting requirements for health and safety incidents.

Key definitions

BLS – Basic Life Support
Primary Care – Airway, Breathing, Circulation and Resuscitation
CPR – Cardio Pulmonary Resuscitation
AED – Automated External Defibrillator

Further research

- NCEMA First Aid Guide
- Skills for Care UK – Basic Life Support Standard
- St John Ambulance – www.sja.ork.uk

Module 2
Fire Safety

Module 2
Fire Safety

Qualification Link

Units
- Nil

Learning outcomes
1. Nature and causes of fire
2. Classification of fires
3. Methods of fire spreading
4. Firefighting equipment
5. Responding to fires

Fire does not respect anything or anyone. It kills, destroys, maims, scars and can leave people jobless if their place of work is destroyed by fire.

Key information

- A fire can double in size every 40 seconds
- Average response time within UAE is 10 – 15 minutes
- 25% of fires in the UAE are attributed to smoking cigarettes

Figure 5 - Oil storage fire

2.1. Nature and causes of fire

2.1.1. The fire triangle

For a fire to start, three things must be present. These three things form a combination known as the fire triangle. The three components are:

- Heat
- Fuel
- Oxygen

If each of these components combine in sufficient quantities, a fire will result. This process is called combustion.

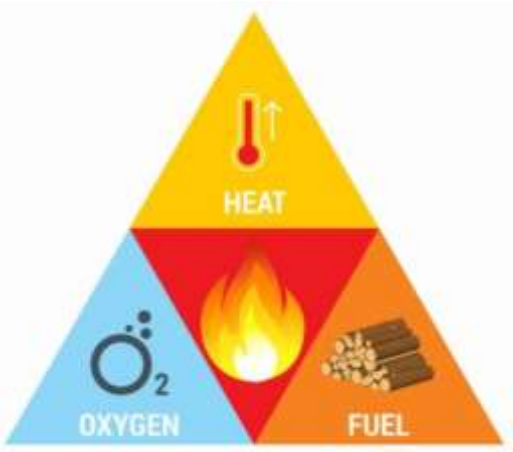


Figure 6 - Fire triangle

Topic focus

Heat

Heat is the source of ignition, and can be anything that gives off enough heat to start a fire. For example:

- **Electrical sparks**
- **Welding sparks**
- **Oven or stove top**
- **Flame**
- **Embers or coals**

Heat can also be produced by friction between surfaces.

Fuel

This can be any combustible material and could be solids liquids, vapours or gas. Examples of fuel could include:

- **Wood, paper, cardboard**
- **Furniture**
- **Petrol, oil, lubricants**
- **Methane, butane or propane gas**
- **Plastics**
- **Fabrics**

Oxygen

This element is simply the presence of oxygen supplied by the surrounding air. If the oxygen is used up through burning, the fire will go out.

Figure 7 - Smothering a fire

2.1.2. Controlling fire

There are three methods of controlling a fire, which are:

- **Starving – This means to remove the source of fuel from the fire**
- **Smothering – This is restricting oxygen from accessing the fire**
- **Cooling – This is removing the heat from the fire**

The process of starving, smothering or cooling a fire is removing 1 element of the fire triangle and causing the fire to stop.

2.2. Classification of fires

Types of fire are classified according to the source of fuel. Knowing the classification of fire is important as it will guide you in choosing the correct method to control the fire.

2.2.1. UAE Classes of fire

- **Class A** – Solid materials (E.g. Wood, paper, fabric, plastic)
- **Class B** – Liquid (E.g. petrol, oil, grease, paint, kerosene)
- **Class C** – Gas (E.g. methane, butane, propane)
- **Class D** – Metal (E.g. sodium, potassium, aluminium, magnesium)
- **Class E** - Electrical

2.3. Methods of fire spreading

There are 4 methods that a fire can spread, given there is sufficient heat, fuel and oxygen to support continued burning. The methods can be described as follows:

2.3.1. Convection

As a fire burns, hot gasses will rise and collect in contained spaces, and if hot enough will cause further fire to start. This process also sends cooled gas (oxygen) downward to the source of the fire, enabling it to continue burning.

2.3.2. Conduction

Heat can transfer through solid materials, eventually increasing the temperature enough to cause combustion of new fuel. A good example of this is if a metal rod were left with one end in a fire, eventually the whole rod would be very hot. In a large fire, this can cause heat to transfer along piping, metal frameworks and other conductive materials causing the spread of the fire.

2.3.3. Radiation

Heat can be transferred through the process of radiation. This means that energy in the form of heat is passed through the Infra-red spectrum. The best example of radiation heat transfer, is heat from the sun. Similarly, a fire can radiate heat outward eventually causing materials (fuel) to ignite and burn.

2.3.4. Direct burning

Heat from a flame or coals can be spread through direct contact with materials. An example of this would be a lit cigarette being dropped into a rubbish bin, causing the embers to contact papers or other materials and resulting in ignition and a fire.

Knowledge of these methods for fire spreading can assist you in identifying fire risks before a fire starts, and also containing a fire that has already started.

2.4. Firefighting equipment

Firefighting equipment can be divided into 2 categories, portable and fixed. Security staff will usually use portable equipment to fight a fire, while emergency services and civil defence would access fixed equipment. Examples of portable equipment include:

- Fire extinguisher
- Fire blanket
- Fire bucket (sand, powder or liquid)

Examples of fixed equipment include:

- Sprinkler systems
- Hose reels
- Hydrants

Key definitions

Co2 – Carbon Dioxide

DCP – Dry Chemical Powder

!!! – Danger, do not use

2.4.1. Extinguishers

The primary uses of a fire extinguisher are:

- To control small fires
- Protect evacuation routes that a fire may block

Attempting to use a fire extinguisher to control a large well established fire will only place yourself into danger

The most common equipment available is the fire extinguisher, and these have been developed to fight specific classifications of fire. Remembering the fire classification system, the following extinguishers are used to control these types of fire:

Extinguisher type				Fire type	
DCP	Co2	Foam	Water		
✓	×	✓	✓	Solid	A
✓	✓	✓	×	Liquid	B
✓	✓	×	×	Gas	C
✓	×	!!!	!!!	Metal	D
✓	✓	!!!	!!!	Electrical	E

Figure 8 - Extinguisher classification

Safety!

- Never use water on a flammable liquid fire – it will spread the fire
- When using foam to fight fat or oil fires, aim to the side and allow the foam to spread over the base of the fire
- Co2 is compressed gas and will blow solid fuels around, spreading the fire
- Never use a fire extinguisher on a person

Figure 9 – Common fire extinguisher types

Key information

- Extinguishers control a fire by **Smothering** or **Cooling** the fire
- All extinguishers have a pressure gauge **except** for Co2
- The contents of a fire extinguisher is known as the **Agent**

One of the duties of security staff is to know the locations of fire extinguishers, and to inspect the condition of them on a routine during patrols.

Things to look for when inspecting a fire extinguisher include:

- Visible damage to the cylinder or valves
- Last technical inspection, and next due date
- Correct pressure reading on the gauge
- Agent label clearly marked and facing out

Any issues identified with fire extinguishers should be immediately reported for action and follow up.

Effective range	Colour	Extinguisher
10-12 meters		Water
3 meters		Foam
1-3 meters		Co2
2-6 meters		DCP

Figure 10 - Color code and range of extinguishers

Topic focus

Using a fire extinguisher

To use a fire extinguisher to fight a fire, the following method has been developed and is taught globally to ensure reliable results during an emergency.

Pull – pull the safety pin from the lever of the extinguisher

Aim – direct the nozzle or spout toward the base of the fire

Squeeze – activate the trigger of the extinguisher

Sweep – move the stream of extinguisher from side to side

This is called the **PASS** method of extinguisher operation.

Safety!

- Keep your hands clear of the nozzle when using Co2 extinguishers, as the compressed gas is -78 degrees Celsius and will cause serious damage to skin

2.4.2. Fire blankets

These items are common in the workplace, and are often found in kitchens. A fire blanket is made of non-flammable fibres, and will not burn. The fire blanket controls and stops a fire through the method of smothering – reducing oxygen access to the fire. To use a fire blanket, take the following steps:

- Remove the blanket from its pouch
- Grip the blanket at the corners, with your fingers behind the blanket for protection
- Place the blanket directly over the source of the fire
- Keep your head behind the blanket to protect against heat and flames

Key information

- A fire blanket will take time to smother the fire and prevent further oxygen from accessing the fire. Once the blanket is in position, do not move it.
- Once a fire blanket has been used, it must be replaced by a new one.

Figure 11 - Fire blanket

Fire blankets can be used to smother a person who is on fire. If a person is on fire, instruct them to:

- Stop – don't run away
- Drop – fall to the ground
- Roll – this will help to smother fire

You can use a fire blanket and wrap it around a person to help stop the fire. In addition to this, a fire blanket can be used to protect yourself from direct burning during an emergency evacuation.

Extinguishers and blankets are the most common form of portable firefighting equipment, and as a potential first responder to fire, you must be confident in their use.

2.5. Responding to fires

2.5.1. Alarms and sensors

In order to comply with the UAE Fire Code, buildings and sites will be fitted with fire alarms and sensors. As security staff, you will be on site 24/7 and are responsible for the immediate response to fire alarms.

The site you are responsible for may also have a security control room equipped with a fire panel from which you can determine the location of activated sensors. Standard Operating Procedures for your site will describe the actions that must be taken regarding the operation of fire alarm panels, however a basic process can be referred to here.

Topic focus

Responding to alarms

1. **When a fire alarm sounds open the panel door, this will stop the internal alarm bell.**
2. **Press the alarm acknowledge button**
3. **Read the information displayed about where the sensor has detected fire or smoke**
4. **Refer to the building layout and position of sensors**
5. **Confirm the presence of a fire by dispatching personnel, or using CCTV to observe the area**
6. **If a fire is confirmed, activate the building alarm and initiate emergency response procedures**

Figure 12 - Fire control panel

Key definitions

Control Panel – The central user interface used to administrate installed fire alarm and sensor systems. Depending on the model, it can also control sprinklers and other fire suppression systems.

CCTV – Closed Circuit Television

Key information

- **When a fire emergency has been dealt with, the control panel must be reset in order to resume normal operation**
- Seek out training on the specific fire control systems installed at your site or building

2.5.2. Discovery of a fire

If you discover a fire, it is important that you are able to respond quickly and responsibly. A standard method of responding to fire has been developed and can be summarised as:

- **Rescue** any person from the immediate area
- **Alert** others – pull the alarm and call 999 or radio the control room and inform the operator. Shout "Fire, Fire, Fire".
- **Confine** the fire – close any doors
- **Extinguish** – use the appropriate extinguisher if the fire is not presenting a threat to life

This system of response is known as **RACE**. Security staff must be aware of manual alarm locations, emergency exits, escape routes and extinguisher locations. Regular revision of this information will provide the best chance of a successful response to fire.

Safety!

Before attempting to fight a fire, ensure that:

- Your escape route is not blocked
- All personnel are clear of the immediate area
- A general evacuation is already underway
- Activate a test burst from the extinguisher before approaching the fire

Assume that you will fail, and be prepared to escape!

2.5.3. Emergency Evacuation

In the even that an emergency evacuation is required, success depends on preparation and awareness, and the following points must be considered:

- Escape routes
- Assembly points
- Evacuation Signs and lighting
- Hydrant and hose access points
- Drills for all staff
- Warden roles
- Controlling re-entry

Security staff will be responsible for coordinating the calm and controlled evacuation procedure, and it is vital that you are familiar with the emergency

evacuation plan. When directing others during an evacuation of your area, follow this guide:

- Give clear and calm direction to leave the area by the designated escape route, confirming that it is not blocked by the fire or other hazards
- Search all rooms and toilets within the area of responsibility
- Ensure there is assistance given to people of determination
- Ensure all doors and windows are shut when leaving each area
- Carry out a roll call at the assembly point using attendance or access registers

  Note: Roll call will not be possible at sites with unrestricted public access e.g. malls, hospitals etc.

- Prevent personnel from attempting to leave the assembly point
- Clear access for Civil Defence to approach and deploy at the site

Figure 13 – UAE Civil Defence fighting a fire

2.5.4. Exits, routes and assembly points

It is very important that emergency exits are clearly marked, and kept free from obstructions. In the event that people need to evacuate, a poorly maintained, or blocked exit could result in injury or death. Security staff must support workplace health and safety officers in monitoring and reporting the status of emergency exits, signs and lighting.

Key definitions

Assembly point – The area designated to evacuate to in the case of an emergency

Arson – Deliberate criminal act of starting a fire

Figure 14 - Emergency exit signs

Planning for emergency evacuation will involve the identification of routes to be taken, and these routes must remain clear of obstruction and potential hazards at all times. When choosing an assembly point, the following should be considered:

- Large enough to accommodate all personnel
- Far enough from the building or site to prevent injury from falling objects, propelled objects and radiated heat
- Clearly marked

Security staff should inspect assembly points occasionally to ensure they are marked clearly, and free of hazards or obstructions

Figure 15 - Assembly point sign

2.5.5. Security vigilance

The primary duty of security staff is to protect people, property and information. Not all fires are accidents, and may be set deliberately by those wanting to cause harm to an organization or its people. Security staff must always remain vigilant to the threat of fire that may be deliberately started. Obvious indicators to look for include:

- People carrying means to start a fire
    - Lighters or matches
    - Fuel in containers
    - Fuel soaked cloth or rags
- Suspicious activity
- Tampering with fire alarms and sensors
- Specific threats made to an organization

Further to the threat of arson, is the risk of looting or theft during or immediately after a fire emergency. Criminals may attempt to take advantage of confusion caused by a fire and commit the theft of property or information. Immediately following an evacuation, security staff should remain vigilant to the risk of theft, and ensure that physical security is maintained at the site.

Further research

- UAE Civil Defence
- National Crisis & Emergency Management Agency – NCEMA
- NAFFCO fire safety tips: https://www.naffco.com/uae/en/fire-safety-tips

Revision questions

1. On average, what is the response time for Emergency services in the UAE?

2. What is the process for using a fire extinguisher?

Hint: PASS

3. How quickly can a fire double in size?

4. What does RACE mean when discovering a fire?

5. What percentage of reported fires in the UAE are started by cigarettes?

6. True or false? A fire blanket is a safe method of controlling a person on fire.

7. What are the 3 parts to the fire triangle?

8. After conducting a roll call at the assembly area, what is the next priority for security staff?

9. What are the 3 methods of controlling a fire?

10. What type of fuel belongs to a Class B fire?

Module 3
Health and Safety

Health and Safety - OHS

Qualification Link

Units

- HLT03009NU17-Identify Hazards in the Workplace

Learning outcomes

1. Identify hazards in the workplace
2. Outline methods of identifying hazards
3. Assess risks of workplace hazards
4. Recommend control measures to minimise risk

There are laws and regulations that govern health and safety in the workplace. Security staff must have a working knowledge of the Occupational Health & Safety requirements in order to support the organisational management with compliance, and to ensure a safe working environment.

Key information

- In Abu Dhabi, **OSHAD** is the governing body for health and safety
- Identification and reporting of hazards by **everybody** is key to achieving health and safety success
- A **hazard** is something that has the potential to cause harm

3.1. Hazard Identification

Security staff conduct site patrols, and frequently inspect 100% of a work area for security purposes. This level of awareness of what is happening within the work site can provide an excellent opportunity to contribute to the identification of hazards. Security staff should always be looking to identify any thing that could cause harm.

3.1.1. Categories of hazard

Hazards can be grouped into categories according to the method in which they could cause harm. The following list describes hazard categories:

- Slips, trips and falls
- Falling objects
- Collision with objects
- Trapping between objects
- Manual handling
- Machinery and Vehicles
- Electricity
- Hazardous substances
- Fire and explosion
- Noise and vibration
- Psycho-Social

These 11 categories can contain a wide range of hazards, and are a good reference point to ensure that when inspecting a workplace, all the possibilities have been considered.

3.1.2. Common workplace hazards

Personal knowledge and awareness will help in the identification of hazards, and the following list is a good starting point:

Slips, trips and falls

- Wet surfaces
- Loose cables or wires
- Uneven surfaces
- Change in level (stairs, walkways etc.)
- Inappropriate footwear

Falling objects

- Ladders or scaffolding
- Poorly constructed materials
    - Bricks, tiles & glass
    - Roofing material
    - Gutters and water pipes
    - Air conditioning fittings
- Equipment and tools

Collision with objects

- Walking into furniture
- Low hanging structures
- Protrusions along a pathway

Trapping between objects

- Door and doorframe
- Caught in machinery
- Gym equipment

Manual handling

- Lifting objects
- Pushing or pulling
- Throwing

Machinery and vehicles

- Workshop tools
- Office equipment (printers, shredders etc.)
- Industrial machines
- Cars and Motorcycles
- Trucks and buses
- Forklift, bulldozer and crane

Electricity

- Overloaded power sockets
- Inappropriate voltage for equipment
- Faulty installations
- Wear and tear of wiring
- Overhead power lines

Hazardous substances

- Cleaning chemicals
- Pool maintenance chemicals
- Pesticides
- Landscaping chemicals
    - Fertiliser
    - Weed killer
- Paints and solvents
- Petrol, oil and diesel

Fire and explosion

- Poor storage of flammable liquids
- Ventilation of flammable vapours
- Pressurised gases
- Incorrect use of appliances (e.g. microwave)

Noise and vibration

- Loud machinery
- Long exposure to high noise levels
- Interfering with hearing (e.g. safety signals or warnings)
- Vibration of hand tools – impact on body
- Vibration of equipment – causing objects to become loose

Psycho-Social

- Stress
- Violence
- Drug or Alcohol abuse

Each of these categories, and any associated hazards should be considered when inspecting a workplace for hazards.

3.2. Workplace inspection

In order to identify hazards, security staff should conduct a thorough inspection of their workplace. The primary responsibility for the management of health and safety will fall to an OHS manager, however security staff are a key contributor to the identification and reporting of hazards within their areas of responsibility.

3.2.1. Methods of hazard identification

Topic focus

Workplace inspections

There are a variety of methods that Security staff can carry out a workplace inspection to identify hazards. These can include:

- Walking around for visual inspection
- Reviewing incident and near miss records
- Work task analysis
- Reading material safety data sheets (**MSDS**) and manufacturer's instructions
- Knowledge of legal requirements

Carrying out a workplace inspection for hazards is the first step in conducting a **Risk Assessment**.

Key definitions

- **Near miss** – An unplanned, undesired event that has the potential to cause injury, damage or loss but does not do so.
- **MSDS** – Material Safety Data Sheet is a summary of the harmful substances contained with a chemical or other material and the exposure required to cause damage. It will also contain recommended treatment if exposed.
- **Risk Assessment** – A methodical examination of what could cause harm to people, and evaluation of how hazards could be controlled

3.3. Risk assessment

Risk assessments are generally required to be completed by designated health and safety officers however, as Security staff are closely linked with the safety and security of a workplace, it is beneficial to have a thorough understanding of the risk assessment process. This will enable either a detailed contribution to a risk assessment carried out by others, or the ability to produce a risk assessment of their own.

3.3.1. Steps of a risk assessment

Key information

There are **2 primary methods** of risk assessment, and the description of each refers to the method of evaluating the risk. They are:

- **Quantitative**
  The likelihood and impact of a risk occurring are calculated using statistical data and historical records. The main feature of quantitative data is that it numerical
- **Qualitative**
  The likelihood and impact of a risk occurring is described using a defined scale of measurement. E.g. the likelihood of a safety incident occurring described as "very low" is defined as 1 time per year.

The **5 steps** of a risk assessment are:

1. Identify the hazards
2. Who could be harmed, and how
3. Evaluating risks and control measures
4. Record and apply the recommendations
5. Review and update if required

(OSHAD-SF, 2016)

Key definitions

- **Risk** – Is the likelihood of harm, and how severe the outcome is
- **Severity** – A scale used to describe the consequences of harm taking place
- **Likelihood –** The probability of harm taking place
- **Risk Calculation** – A formula used to evaluate risk (Likelihood x Severity = Risk)

The complete process of conducting risk assessments could be described as a cycle, due to the continual monitoring and updating of information.

Figure 16 - Risk assessment method

3.3.1.1. Step 1 – Identify the hazards

This process involves listing of all hazards identified through the process of workplace inspection, and considering all categories of hazard. The use of a standard template will help with ensuring that enough detail is recorded.

For example:

Location	Category	Hazards
Main office	Slips & Trips	Computer cables
		Loose carpet
		Steps down to foyer
	Electrical	Overloaded sockets
	Stress	Crowded space

Figure 17 - Hazard identification table

A deliberate and methodical inspection of the workplace and recording of hazard details, will ensure that the next steps can be completed accurately.

3.3.1.2. Step 2 – Who can be harmed?

The purpose of this step is to assess who will likely come into contact with the hazards identified, and how it could harm them. This step will provide vital information used in step 3. A general guide to the types of people includes:

- Workers
- Contractors
- Visitors
- Public
- People of determination

For example:

Hazards	Who can be harmed?	How?
Overloaded electrical socket	Office Workers	Are close to equipment that may short circuit and burn
	Contactors	May perform maintenance on equipment and be electrocuted

Figure 18 - People at risk table

The process of assessment will finish with a clear understanding of the hazards and how they could impact each person at risk within the workplace.

Topic focus

Recording hazards and people at risk

- Consider all of the hazard categories, and methods of identification
- Be thorough and methodical
- Use a standard template to make sure enough information is collected

3.3.1.3. Step 3 – Evaluate risks and control measures

Evaluation of risk is a critical step in the assessment process, and will guide the decision making process for controlling risks. The outcome of evaluating a risk is known as a risk score.

Likelihood x Severity = Risk Score

In order to evaluate the risk that a hazard presents, the method must be chosen – Quantitative or Qualitative. The availability of data will most likely determine which method of evaluation is chosen. Often, there is not enough recorded numerical data to properly evaluate risks using a Quantitative method, therefore Qualitative evaluation will be required using defined scales to describe the likelihood and severity of hazards causing harm.

A useful tool to assist with this process is called a risk matrix. The risk matrix describes likelihood and severity, and provides a score to allocate to a hazard based on the evaluated Likelihood and Severity.

For example:

Risk Score		Likelihood				
		1	2	3	4	5
Severity	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Risk Scale	
20-25	Very high
15-19	High
10-14	Moderate
5-9	Low
1-4	Very low

Figure 19 - Risk Matrix

To evaluate a risk, existing control measures for each hazard should be identified, and the reduction of risk that is provided by the control measure should be taken into consideration when calculating the risk.

Key information

The established method of applying control measures to a hazard is known as the **Hierarchy of Control**. There are 5 levels to the hierarchy and can be applied in the following order of most to least effective:

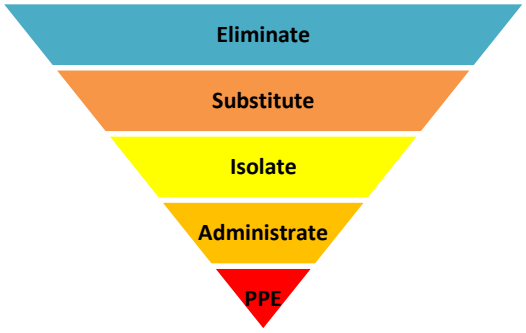


Figure 20 - Hierarchy of controls

Wherever possible, the hierarchy of control should be applied in the order to most effectively reduce the risk of a hazard.

Key definitions

- **Risk Matrix** – a grid of risk scores, based on likelihood and severity of hazard causing harm

Hierarchy of controls:

- **Eliminate** – remove the hazard completely
- **Substitute** – replace the source of the hazard
- **Isolate** – Guard or control the hazard
- **Administrate** – change policy or procedures
- **PPE** – Use protective safety equipment

With this knowledge, it is possible to continue the process of risk assessment, identifying control measures and making recommendations.

For example:

How?	Existing controls	Recommend
Are close to equipment that may short circuit and burn	None	Engineering: Install additional power outlets for office equipment use

May perform maintenance on equipment and be electrocuted	Administrative: Site policy for contractors to be aware of hazards	Engineering: Install additional power outlets for office equipment use

Figure 21 - Risk control measures

Topic focus

Evaluating risk

With the hazards, people effected, existing controls and recommendations identified, the likelihood and severity of harm occurring can be evaluated. Using the most practical method – Quantitative or Qualitative, evaluate the risk for each hazard.

- Use available sources of information to make an accurate evaluation of the likelihood and severity
- Calculate a risk score for each hazard

For example:

Likelihood (1-5)	Severity (1-5)	Risk Score (1-25)	Risk Level
1	4	4	Very Low
2	5	10	Moderate

Figure 22 - Risk evaluation

A completed view of the risks within the workplace can now be seen. Turn to the following page for a completed example of a workplace risk assessment.

Risk Assessment Worksheet										
Location	**Category**	**Hazard**	**Who can be harmed**	**How**	**Existing Controls**	**Recommendations**	**Likelihood**	**Severity**	**Risk Score**	**Risk Level**
Security office	Slips, trips and falls	Loose carpet in entrance	Workers, Contractors	Foot caught in carpet. Falling to floor	None	Substitute: replace the carpet with new	3	2	6	Low
		Loose projector cables	Workers	Tripping on cable, falling to floor	None	Isolate: Install cable guides to route the cords and keep tidy	2	2	4	Very low
	Collision with objects	Duty officer desk protrudes into walk path	Works, Contractors	Walking into corner of the desk	None	Isolate: Relocate the desk out of the way	3	2	6	Low
	Manual handling	Extended use of CCTV systems	Workers	Repetitive task	Administrative: Scheduled breaks	Substitute: Get new workstation that is adjustable for each user	4	3	12	Moderate
	Electricity	Poorly maintained lights	Workers, Contractors, Public	Fusing of light installation causing electrical fire	None	Substitute: Replace the lighting system	3	5	15	High
		Exposed fuse box	Workers, Contractors, Public	Live electrical wires protruding – Electrocution	None	Substitute: Replace the housing and ensure access is controlled	4	5	20	Very High
	Hazardous substances	Cleaners using air freshener	Workers, Contractors, Public	Asthmatic reaction to aerosol spray	None	Administrative: Policy for use in accordance with MSDS	2	5	10	Moderate

Figure 23 - Completed risk evaluation table

Practice Activity

Given the following information, complete a Risk Assessment Worksheet

Sample Incident Log

Workplace:	Vehicle entry control point at an oil refinery site
Duration:	1 Year

Incidents	**Description**	**Severity**		
		No treatment	Minor treatment	Severe - Hospitalisation
25	Dehydration and dizziness reported by workers	5	10	10
3	Staff hit by vehicle during duty	0	0	3
2	Public hit by vehicle inside the control point	0	2	0
5	Staff burned by boiling water in the coffee room	0	4	1
30	Public hit by closing access barrier	10	20	0
3	Staff electrocuted by radio charging station	0	3	0
15	Staff slipped on leaked oil from vehicles while on duty	0	13	2
2	Staff burned by vehicle fire attempting to extinguish	0	2	0
1	Contractor fell of roof during maintenance	0	0	1

Risk Assessment Worksheet

Location	Category	Hazard	Who can be harmed	How	Existing Controls	Recommendations	Likelihood	Severity	Risk Score	Risk Level

Key information

Foundational skill

- A good understanding of the concepts involved in completing a risk assessment for hazards in the workplace will benefit security staff as they continue to develop in their careers.
- The basics of likelihood and severity assessment can be applied to security threat assessments, and these skills will serve the security professional well during their career.

Figure 24 - Hazard recording

3.3.1.4. Step 4 – Record and apply recommendations

The identification of hazards and control measures is only useful if they are recorded and the recommendations are implemented. It is important to note, that even if control measures are applied, it is impossible to completely eliminate risk if the hazard still exists. The remaining risk is known as "Residual Risk", and this level must be tolerable to an organisation and the legal standards.

Key information

As Low As Reasonably Practical

- There is a concept of reducing existing risk to a level that is as low as reasonably practical (**ALARP**)
- If the following 3 things are reasonably practical, then the option to reduce risk should be taken:
    - **Time**
    - **Money**
    - **Effort**
- Reasonably means different things to different organisations. This should be considered when deciding how to proceed with control measures.

Using the risk assessment produced in the previous step, a risk assessment report can be completed and distributed to all persons as required. Rarely will Security staff be required to coordinate the application of the recommendations that are made, however they may be consulted by health and safety managers during the implementation process. It is good practice to understand the risk assessment report writing method, and the basic format can be outlined as:

- Report Number
- Date
- Valid until
- Department or work area
- Key risks
- Other risks & ratings
- Relevant policies and procedures
- Risk assessment summary
- Record keeping requirements
- Name of person completing

An example can be found on the following page, and the opportunity to practice completing a risk assessment report is given.

Risk Assessment Report					
Number	01	**Date**	1-1-2019	**Valid until**	1-6-2019
Department / Work area		Entry control point 1			
Duties description in the workplace		▪ Traffic management ▪ Access control ▪ Searching vehicles ▪ Searching people			
Key risks identified		1. Heat and dehydration is highly likely 2. Vehicle accidents have severe impact 3. Access control mechanisms interfere with public safety			
Risk assessment findings		**Risk rating**			
1. Environmental		High			
2. Collision with objects		High			
3. Slips, trips and falls		Moderate			
4. Machinery and vehicles		Moderate			
5. Electricity		Low			
6.					
7.					
8.					
9.					
10.					
Relevant policies & procedures		1. Security duty instructions 2. OSHAD-SF-CoP 44.0 - Traffic Management and Logistics 3. OSHAD-SF - TG - Safety in the Heat v3.0 4. OSHAD-SF-CoP 15.0 - Electrical Safety v3.1			
Risk assessment summary		The workplace inspection was carried out by reviewing incident records, and conducting a walk around of the work location to identify hazards present. The duty instructions for staff were reviewed, and relevant health and safety policies were referred to. The risks that have been identified will require treatment, and those that have been scored as moderate and higher should be prioritised for immediate action.			
Record keeping requirements		1. File in departmental health and safety records 2. Communicate findings to all staff			
Completed by		Person One			

Figure 25 - Example risk assessment report

Risk Assessment Report					
Number		**Date**		**Valid until**	
Department / Work area					
Duties description in the workplace					
Key risks identified					
Risk assessment findings		**Risk rating**			
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
Relevant policies & procedures					
Risk assessment summary					
Completed by					

3.3.1.5. Step 5 – Review and update

A risk assessment should be reviewed should any change to the work area take place. This could include any of the following areas:

- New laws or regulations passed
- New materials or substances in use
- A change in work policy or procedure
- Installation of new equipment
- New personnel
- Any accident or near miss occurs

Regular review and update of the risk assessment will ensure that hazards are controlled to a level that is as low as reasonably practical.

3.4. Risk reporting requirements

3.4.1. General reporting requirements

According to the OSHAD Systems Framework, each step of the risk assessment process is required to be recorded. Any methods and sources of information must also be recorded. This ensures that legal and organisational requirements are covered, and the benefits of re-using information can be achieved.

Larger or more complicated organisations will maintain a risk register, that tracks all risk assessments that have been produced, and can be used to monitor and update the risk assessments. (OSHAD-SF, 2016)

3.4.2. Incident reporting

All health and safety incidents are required to be recorded by an organisation, regardless of the severity. Certain incidents are "reportable" given the seriousness and severity of the incident. OSHAD requires that the following types Dangerous Occurrence:

Incident Type	Time
Explosion or fire	3 days
Collapse of equipment	3 days
Machinery damage	3 days
Electric lines, cables & pipelines	3 days
Malfunctioned radiation equipment	3 days
Spilled flammable liquids and gases	3 days
Release of hazardous materials	3 days
Release of Biological agents	3 days
Contaminated needle injury	3 days

Figure 26 - Reportable occurrences list

The following injuries must also be reported to the sector regulatory agency:

Incident Type
Injured and unable to perform work
Fractured bone
Loss of any body part
Loss of consciousness
Serious head injury
Serious eye injury
Exposure to hazardous substance
Separation of skin from underlying tissue
Electrical shock
Serious burns
Entrapment of a body part in machinery
Spinal injury
Dislocation of a joint
Loss of bodily function
Serious laceration

Figure 27 - Reportable injuries list

Further detail can be found within OSHAD-SF Mechanism 11 – Incident notification.

3.5. Working in the heat

3.5.1. Heat injuries

The UAE experiences extreme heat during the summer months, and staff who are exposed to these conditions may experience heat injuries, causing a loss of organisational capability. The following are a list of possible injuries caused by extreme heat in the working environment:

- **Heat rash** – skin irritation caused by sweating and hot, humid weather
- **Heat cramp** – caused by loss of salt in the body through sweating
- **Fainting or dizziness** – can be caused by prolonged standing, with poor hydration
- **Heat exhaustion** – Excessive sweat loss and exhaustion, very weak and dizzy.
- **Heat stroke** – Very serious condition, when the body can no longer control its own temperature through sweat. Death can result without proper treatment.

3.5.2. Prevention of heat related illness

There are several strategies that can be used to help prevent heat injuries. The most common may include: (OSHAD-SF, 2016)

- **Acclimatisation** – slowly becoming accustomed to working in a hot environment
- **Hydration** – continuing to drink water throughout the day (4-6 litres per day)
- **Limit caffeine** – coffee and other drinks containing caffeine can cause further dehydration
- **Monitor hydration levels** – Urine colour can indicate hydration, and charts are available to interpret these levels

Figure 28 – Urine colour hydration chart

Security staff may experience long periods of exposure to hot working environments, and must be especially aware of the risks and prevention methods. Close attention should be given to the condition of co-workers, and any concern for their health should be immediately reported and treated.

3.6. Safety signs and symbols

A standard system of signs and symbols has been developed to inform personnel at a site of hazards, safety requirements and emergency locations. The system is colour coded for easy identification and is divided into 5 categories:

Category	Type of sign
E	Escape and emergency equipment
F	Fire safety
M	Mandatory action
P	Prohibited
W	Warning

Figure 29 - Health and Safety sign categories

3.6.1. Escape and emergency equipment signs

These signs are located at emergency exits, and are also used to mark the location of safe areas, evacuation routes and first aid equipment.

Figure 30 - Example escape and emergency equipment signs

3.6.2. Fire safety signs

These signs are used to mark the location of firefighting equipment, or alarm activation points

Figure 31 - Example fire safety signs

3.6.3. Mandatory action signs

These signs show safety precautions that are mandatory when entering an area or using equipment, and they must be followed.

Figure 32 - Example mandatory action signs

3.6.4. Prohibited signs

These signs identify actions or materials that are not prohibited within the area, and must be enforced.

Figure 33 - Example prohibited signs

3.6.5. Warning signs

These signs are used to warn of hazards that are present in the area, and will inform personnel that there is the potential for harm to be caused.

Figure 34 - Example warning signs

Key information

Safety signs

- Will be placed by health and safety officers
- Signs may have additional words to clarify the meaning e.g. “Hearing protection must be worn”
- Security staff must enforce the following of safety signs, as they are responsible for the safety of people.

Health and safety is a broad topic, and the principles of controlling hazards and risks will continue throughout the career of a Security professional. Keeping in mind the presence of hazards, and control measures available will contribute to the success of a safety culture in the workplace.

Further research

- www.oshad.ae
- NCEMA-OHS National Standards
- ISO 31000 – Risk Management
- ISO 45001 – Occupational Health and Safety

Module 3 Revision

Revision questions

1. What are the 5 steps of a risk assessment?

2. How could you perform a workplace inspection for hazards? Give 3 methods:

3. Can you recall 5 categories of hazard?

4. What is the definition of Risk?

5. What are the 2 primary methods of risk evaluation? (Hint: “Q & Q”)

6. What is a MSDS?

7. List the hierarchy of controls:

8. What is the formula for calculating a risk score?

Module 4
Security roles and responsibilities

Module 4
Security roles and responsibilities

Qualification Link

Units
- SEC03001NU18-Demonstrate knowledge of security operations

Learning outcomes
1. Identify laws and organisations that support security operations
2. Identify physical security principles
3. Outline the roles and responsibilities of an individual and a security team
4. Demonstrate security mindedness in the workplace

4.1. Personal values of Security Staff

The nature of performing a security role means that there are certain personal values that will assist Security staff in the performance of their duties.

Key information

FAHR code of conduct

The following values have been identified by the UAE Federal Authority of Human Resources as core to the success of a professional who is dedicated to their work:

- Excellence
- Diligence
- Integrity
- Honesty
- Objectivity
- Neutrality
- Alertness
- Efficiency
- Leadership
- Transparency
- Fairness and Equality

Security staff who pursue these personal values will be well placed to succeed within their chosen profession.

4.1.1. Traits of a Security professional

In addition to any personal values held, there are a set of personality traits that can be developed and will assist Security staff in performing their duties. A Security professional should develop:

- **Curiosity** – Always question why
- **Determination** – Mental toughness to maintain vigilance and withstand long periods of no active risks or threats
- **Communication** – The ability to effectively understand, and be understood
- **Team Work** – A willingness to contribute to collective goals and support others will strengthen the service provided by security staff

4.1.2. Ethics and professionalism

Security staff are in a position to make decisions that may affect a variety of other people, and must be trusted to act ethically and professionally.

Key definitions

Ethics – Moral principles that guide a person's behaviour or activities. The knowledge of what is right and wrong.

Professionalism – The qualities of a professional. This can include:

- Personal appearance
- Reliability
- Competence
- Attitude

Example:

Behaviour that is not ethical could include:

- Letting a member of staff through an access control point without the proper pass, because they are a personal friend
- Listening to, and then passing on details of a private conversation

Behaviour that is unprofessional could include:

- Continually reporting late for duty
- Eating food while positioned at a security checkpoint

Topic focus

Standards of professionalism

The following is an outline of the required standards of professionalism the Security staff should aim to achieve:

- **Personal presentation**

- Personal hygiene is good
- Clothing is clean and pressed
- Footwear is clean and in good condition
- ID and security passes are worn correctly
- Body language is positive and authoritative

- **Equipment**
  - Well maintained and clean
  - Stored correctly when not in use
  - Carried correctly while on duty
  - Secured from the public or potential criminals
- **Attitude**
  - Positive approach to all situations
  - Alert to all activity within the area of responsibility
  - Motivated to achieve excellence through the use of best practices
  - Willingness to solve problems

These guidelines will ensure that a professional image is presented. This by itself can often be enough to stop a potential criminal from acting due to the physical presence of a professional looking Security Team.

4.2. Roles and tasks

Private security staff should be prepared to operate within a variety of different commercial, industrial or public sectors. Awareness of the potential places of employment is important as it will allow the Security staff to be thinking critically about the role of security within each of the potential sectors. The individual roles may also vary depending on the site, client or industry that the Security staff operate in.

4.2.1. Sectors of employment

A summary of the sectors that Security staff may operate in can include:

- Government ministries and buildings
- Airports
- Sea Ports
- National borders
- Critical infrastructure sites
  - Oil and Gas
  - Power generation
  - Water treatment
  - Nuclear facilities
- Shops and Malls
- Industrial plants and zones
- Hospitals & Clinics
- Residential buildings and compounds
- Sporting grounds
- Parks and beaches
- Theme parks and tourist sites
- Cultural centres and museums
- Places of worship
- Special events
- VIP Protection

The effective security of each of these sectors will rely on Security staff applying principles of physical security.

4.2.2. Duties and tasks

Security staff can expect to perform a variety of duties and tasks depending on the client, site, industry sector and threat levels.

Key information

The ministerial decision No. 557 of 2008 outlines seven primary duties:

- Keeping watch over people, property and information
- Protecting people or property from damage or any other illegal activity
- Controlling access to the companies protected
- Preventing the stealing or exploitation of goods, money or other valuables
- Detaining persons who are suspected of committing theft or exploitation of any goods, money or other valuables
- Responding to security alarms
- Maintaining order and safety during sporting activities, concerts and other public events

The basic duties and tasks described can be categorised into the following security roles:

- Access control
- Traffic and parking management
- Searching
- Crowd control
- Patrolling
- Control room operations

Procedures for each of these roles are explained in detail in later modules of the course

Figure 35 - Security access card

4.2.3. Workplace security culture

Security staff have the opportunity to educate and inform colleagues regarding good practice for security in the workplace. This could be something as simple as encouraging others to report suspicious activity, wearing ID, or locking their computers while away from the desk.

Other contributions that Security staff can make toward the workplace security culture include:

- Notifying colleagues of new security risks
- Reinforcing security policies and procedures
- Ask colleagues to confront any person who may not be authorised in the area
- Ask colleagues to be aware of people attempting to follow through locked doors
- Ask colleagues to be aware of suspicious items or packages
- Ask colleagues to monitor and report violent or hostile behaviour within the workplace
- Encouraging colleagues to clear their desks, dispose of documents correctly, and maintain information security procedures
- Encourage colleagues to report lost or stolen access cards and keys
- Ask colleagues to make sure that printers are not left with documents in the tray

There are many factors that contribute to a security culture, and Security staff must always lead by example.

4.2.4. Organisational impact of security

There are many ways that the presence of Security staff can positively impact an organisation and provide benefit to businesses and clients. Examples of this include:

4.2.4.1. Improved organisational resilience

Well trained and confident Security staff will effectively carry out response plans to critical incidents, helping an organisation to maintain business continuity. This means that the primary functions of an organisation can resume as soon as possible, and return to normal operations

4.2.4.2. Peace of mind

A professional security team can reassure workers and clients, allowing them to focus on other areas of an organisation. Staff can happily come to work in the knowledge that any risk to their personal safety is reduced, and business owners can be satisfied that security risks and threats are being monitored and prevented

4.2.4.3. Improved reputation

Security staff can improve the reputation of an organisation through a professional image, excellent customer service and communication, and decisive and effective actions. Organisations can use Security staff as another way of branding and marketing

Key information

- Professional and authoritative Security staff can prevent crime simply by being on duty. This is known as presenting a “hard target”.

Figure 36 - Abu Dhabi Judicial Department

4.3. Laws and regulations

Security staff will be required to act with authority in order to protect people, property and information. The UAE has instituted a series of laws that the Security professional can rely upon when carrying out their duties.

4.3.1. UAE Laws and regulations

Key information

Relevant Laws

- Federal Law no. 37 of 2006 (Private Security Companies)
- Ministerial decision 557 of 2008 (Private Security Companies)
- Federal Law no. 3 of 1987 (The Penal Code)
- Federal Law no. 3 of 2016 (Children's rights)

Specifically written to govern the Private Security industry, Ministerial decision 557 of 2008 is the source of law regarding the operation of a private security company, licensing of security staff and training requirements.

The UAE Penal Code Penal Code is a set of legal provisions that determine the actions which are recognized as crimes and explain the penalties incurred upon them. The Code includes two types of rules:

- general provisions which apply to all/most crimes
- provisions of each individual crime which explain its facts and determine the appropriate penalty.

Topic focus

Detaining suspects

Only law enforcement officials have the legal powers to physically detain a suspect. Security staff may detain a suspect only if they submit to the request. There are 4 main points to follow when detaining a person:

1. Call the police
2. Identify yourself as Security
3. Request that the suspect cooperate
4. Inform the suspect of the reason for detaining them

This procedure applies to suspects who have not been reliably witnessed committing a crime.

Arresting criminal offenders

(Art 48 UAE Penal Procedures Law 35 of 1992)

According to the UAE Penal Code, civilians have the power to arrest a person who has been caught red handed committing a crime. This applies to Security staff, and enables them to restrain and hold a person until the police arrive and take custody.

When arresting a person, you must:

- Witness them committing the crime
- Identify yourself as Security
- Inform the person they are under arrest
- Inform the person why they are under arrest
- Call the police

Use of force

(Ch. 4, Section 1 Article 56 UAE Penal Code)

Use of force is permitted in self-defence when:

- You face immediate danger of a crime against yourself, your property, or the property others and;
- You have no possibility of resorting to the Police and;
- You have no other means of stopping the crime and;
- The use of force is necessary to stop the danger, and is proportionate with the threat being presented

Figure 37 - Child protection Law

Federal Law No. 3 of 2016 is also known as Wadeema Law, and has been written to provide protections for children. Security staff are in a position to observe cases of child neglect, abuse or mistreatment and must understand the principles of child protection. There are many clauses within the Law, but the following may be closely linked to the duties of Security staff:

Chapter 1

- Article 4.2a – Give children priority of protection, care, rescue and guidance in cases of emergency, disaster, armed conflict and any crimes committed

Chapter 2

- Article 14 – It is prohibited for children below age 15 to be employed

Chapter 4

- Article 21.1 – It is prohibited to sell or attempt to sell tobacco products to children
- Article 21.2 – It is prohibited to smoke in public and private transport, and indoor places in the presence of a child
- Article 21.3 – It is prohibited to sell or attempt to sell alcohol to children

Security staff should always be aware of the welfare of children, and make sure to act in the best interests of children

Key definitions

Child – A person who is under 18 years' old

Red handed – Crime directly witnessed by a person

Self-defence – Use of force to protect yourself from harm

Offender – A person that commits a crime, or misdemeanour

4.3.2. Security Organisations

Within the UAE there are several organisations that represent the security hierarchy within the country. Security is organised according to the following structure:

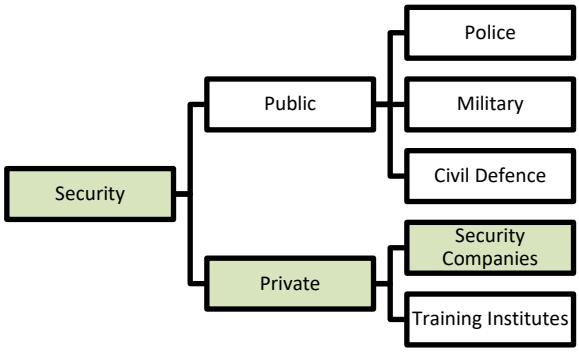


Table 1 - UAE Security Organisations

These organisations are governed by various Ministries or Departments according to their place within the hierarchy. Private security is regulated by 2 organisations within the UAE:

Table 2 - Private Security Regulation, Abu Dhabi & Northern Emirates

Dubai

GOVERNMENT OF DUBAI

Security Industry Regulatory Agency

Table 3 - Private Security Regulation, Dubai

All private security companies and commercial activity within the Security industry are governed and regulated by these departments.

4.3.3. Licensing and inspection

Security staff are issued licenses to work, and these licenses are provided by the Private Security Business Department in Abu Dhabi and the Northern Emirates, or the Security Industry Regulatory Agency in Dubai.

PSBD	SIRA
Event Security Guard	Security Consultant
VIP Security Guard	Security Expert
Critical Infrastructure Security Guard	Security Trainer
Airport Security Guard	Head of Security
Hospital Security Guard	Security Manager
Bank Security Guard	Head of Security Operations
C-I-T Security Guard	Security Supervisor
Security Guard	Security System Engineer
Security Supervisor	Security System Inspector
Security Manager	Security System Technician
	Money Transport Guard
	Security Guard
	Money Transport Vehicle Driver
	Security System Operator
	Event Security Organiser
	Watchman

Table 4 - UAE Private Security License Categories

In order to apply for a license to work within the security industry, applicants must meet a range of requirements that are set out by the concerned authority.

Key information

Detailed information regarding eligibility can be found in on the PSBD and SIRA websites, however to apply for Security Guard license the following criteria must be met:

PSBD - Abu Dhabi & Northern Emirates

- Able to speak both Arabic and English, and master either one, with a working knowledge of the other
- Hold a high school diploma, or equivalent
- 2 years of experience in the police or armed forces
- Aged between 21 and 55 years
- Over 160cm in height (150cm for females)
- Body is well proportioned and fit
- Body is free of all defects
- Must pass the tests set by the concerned authority

(Law 557 of 2008, chapter 6, article 96)

SIRA - Dubai

- Age between 21 and 55 years
- Physically and mentally fit
- Arabic or English communication skills
- Valid passport and visa
- Good conduct certificate
- Passport sized photo
- Security course certificate
- Fitness certificate

(Resolution 1 of 2018, Article 15)

As Security staff progress through their careers, new licenses will be required according to the position and role held.

Private security companies are also licensed and regulated by the concerned authorities. Laws and

regulations are enforced, and inspections are carried out to ensure compliance with regulations. Private security companies, and Security staff must comply with inspection teams and requests from the PSBD.

Key information

Licensed Security staff must be wearing an approved uniform, that will display:

- Name of the company in Arabic and English
- Company logo
- Security license issued
- Company ID card

Security staff must also carry:

- A communication device
- 2 Black pens
- A notebook

4.3.4. Staff & employer rights

The rights of Security staff, and Private Security Companies are protected by the Human Resources law, and the relevant laws governing Private security in the UAE.

United Arab Emirates
Ministry Of Interior
Private Security Business Department

دولة الإمارات العربية المتحدة
وزارة الداخلية
إدارة شركات الأمن الخاصة

Ministerial Decision No. 557 of 2008

The most common staff rights that are described include:

- Monthly salary of not less than 6000AED
- Working day not more than 9 hours
- Working week not more than 6 days
- 1 month paid vacation per year

(Ministerial decision No. 557 of 2008, Article 34)

UNITED ARAB EMIRATES
MINISTRY OF HUMAN RESOURCES
& EMIRATISATION

الإمارات العربية المتحدة
وزارة الموارد البشرية والتوطين

The most relevant employer rights include the ability to terminate employment contracts if:

- Employee uses false certificates
- Employee is within probation period
- Employee commits an error resulting in massive material losses
- Employee violates safety instructions that are written and posted in the workplace
- Employee fails to perform duties in accordance with the contract, and does not remedy the failure despite a written warning
- Employee sharing of company secrets
- Employee conviction in a crime of honour, honesty or public ethics
- Employee found in a state of drunkenness or under influence of narcotics
- Employee assaults others in the workplace
- Employee is absent without valid cause for more than 20 non-consecutive days in a year, or for more than 7 consecutive days

(Ministerial Decree No. 212 of 2018, Article 120)

The law regarding Private security, employment, crime and self-defence is very detailed. Security staff should take time to read these laws and gain a broad understanding of the legal requirements when working within the industry, and as good citizens of the UAE.

4.4. Principles of physical security

It is essential that Security staff understand the guiding principles of effective physical security. This will enable staff to recognise the elements applied at the site or location for which they are responsible, and also to think critically about how the various principles are interacting and whether or not they are effective.

4.4.1. Layers of physical security

Best practice in designing physical security solutions dictates that the elements of a secure site are "layered" in a specific order, providing depth and further options should a single layer become compromised.

Key definitions

4 Ds of Physical Security

- **Deter** – Discourage potential intruders or attackers from attempting to breach security
- **Detect** – Identify that an intrusion, attack or breach of security has taken place, allowing time to respond
- **Delay** – Increase the time taken for an intruder or attacker to penetrate and reach vital areas or assets within an organisation
- **Deny** – Block physical access to locations or assets

The 4 D's offer a structured way of developing security plans, and have proven effective in the protection of sites. Almost all security systems and

equipment can be categorised according to the 4 D's.

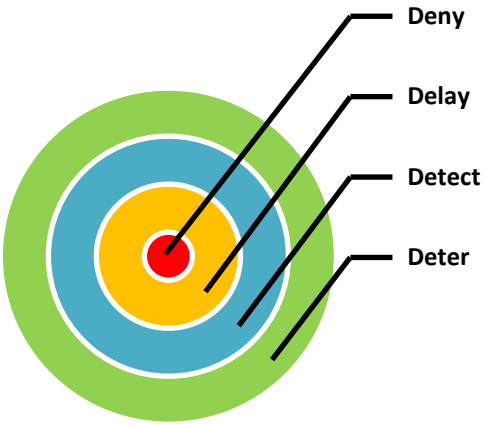


Table 5 - Layers of physical security

Table 6 - 4 D's principles of physical security

Topic focus

The four D's and Security Measures:

Deter – The purpose of deterring crime is to eliminate the need for further response, and is the preferred option. Examples of security measures that can deter a crime from happening include:

- Warning signs
- Brightly lit areas
- Open spaces with good visibility
- Clearly marked perimeter or boundary
- Visible presence of security staff

Detect – Detection of crime, intrusion or attack enables response by Security staff. There are many methods available to enable detection, and may include:

- Security staff on watch
- CCTV systems
  - Pan, Tilt & Zoom Cameras
  - Motion activated
  - Night vision
  - Virtual zone recognition
- Motion sensor
- Alarmed doors, gates, windows etc.
- Perimeter intrusion detection (PID)
  - Thermal sensor
  - Microwave beams
  - Vibration sensors
  - Radio frequency fields
  - Optical fibre cable sensors
- Canine security

Delay – Using smart site design and mixed security access systems will increase the amount of time taken for a criminal to penetrate a site. Examples of this include:

- Lockdown of zones within a site
- Distance between perimeter and vital assets or areas
- Multiple lock types e.g.
  - Physical key
  - Radio Frequency key (Card)
  - Biometric
- Hostile vehicle barriers (HVM)

Deny – This is the ultimate goal of physical security, to deny criminals access to that which the organisation requires protecting. Each security measure works together to deny criminals access to people, property and information

Example of site security measures – 4 D's

Deter	
	Perimeter Fence
	Warning signs
	Security lighting
Detect	
	CCTV
	ID Checks
	Mobile patrols
	Sensors

Delay	
	Locks
	Hostile vehicle barriers
	Layered perimeters
Deny	
	Barriers and access control
	Perimeter Fence
	Physical response
	Landscape design

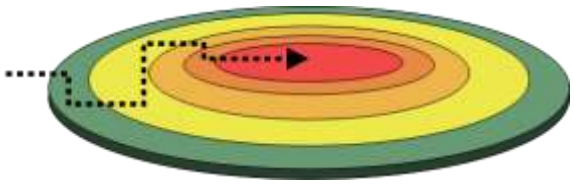


Figure 38 - Hierarchy of 5 zones of control

4.4.2. Hierarchy of zones

In order to achieve a security solution that will still allow for the proper operation of a client site or facility, the concept of zones is applied to determine who can go where, and what security measures are used to enforce each zone.

There are various terms used to describe the hierarchy of zones, with some used specifically for certain industries e.g. banking, cash-in-transit or public health care. A best practice approach is to use the following zones as a guide for levels of security access:

- Public Zone
- Reception Zone
- Operations Zone
- Security Zone
- High Security Zone

The allocation of zones, and access control measures is the responsibility of Security Managers and Organisational Leadership, however Security staff should be aware of the zones operating in their workplace, and the methods used to enforce each zone. This will be covered in further detail in the access control module.

Information sharing

4.5. Police, emergency services and Private Security

There are many departments and services that make up the public security sector, and the appropriate department will respond depending on the security or emergency situation. It is important that Security staff are aware of the different agencies, and how to communicate with them in the event of a safety or security incident. Responsibility for safety and security in the UAE is broadly divided across these organisations:

- Ministry of Defence
- Ministry of Interior
- Civil Defence
- Supreme council for National Security

4.5.1. Agencies responsible for security response

Security staff will cooperate with a variety of public safety and security organisations, and a good knowledge of these organisations will ensure a smooth working relationship.

Key information

The most likely organisations that Private Security staff will cooperate with include:

- **999** - Police
- **998** - Ambulance
- **997** - Civil Defence
- **996** - Coast Guard

شرطة دبي
DUBAI POLICE

شرطة أبوظبي
ABU DHABI POLICE

Police – This is the organisation that Security staff are most likely to cooperate during any security incident. Police are responsible for enforcing the law, and given powers above that of normal citizens. Police will respond to reported crimes arrest offenders, collect evidence, interview witnesses and prepare

Within the police there are several directorates that are tasked to deal with specific incidents or activities. Security staff will simply call **999** to request police, however during the follow up to a security incident, Security staff may deal with Police Officers from the following directorates:

Abu Dhabi & Northern Emirates

- Community policing department
- Correctional and Punishment establishments
- Police follow up and after care department
- Security information department
- Public establishments protection department
- Public order department
- Diplomatic premises protection department
- CID Directorate
- Drug enforcement directorate

- Transportation Infrastructure security department
- Traffic and patrols directorate
- Emergency and public safety directorate
- Crisis and disaster management department
- Ports and Airports security police directorate
- Forensic evidence department
- Crime scene department
- Security inspection department (K9)

Dubai

- General department of criminal investigation
- General department of Anti-Narcotics
- General department of forensics and criminology
- General department of transport and rescue
- General department of protective security and emergencies
- General department of traffic
- General department of airport security
- Ports Police

4.5.2. Working relationships

Private Security staff rely on the police and emergency services to respond to and quickly support them during safety and security incidents. Security staff will support their client organisation and will often observe security incidents and crime before anybody else. Security staff must then escalate the incident to the police in order to allow them to enforce the law.

4.5.3. Information sharing and support

Security staff must be prepared to share relevant details and information with the police when they arrive and take control of an incident. Further details on the procedure for sharing information and cooperating with the police are contained in the module on observation and note taking

Further research

- Ministerial Decision 557 of 2008
- UAE Penal Code
- Abu Dhabi Urban Planning Council - Safety & Security Planning Manual
- ISO 27002 – Information Security - Control 11
- www.government.ae section on handling emergencies
- https://manafth.ae
-

Revision questions

1. What are the 11 values of a professional according to FAHR?

2. Give 1 example of good ethics, and 1 example of bad ethics

3. Can you recall 5 sectors that private security may be employed in?

4. What are the 7 core tasks of private security, according to Ministerial decision no. 557 of 2008?

5. List 3 benefits that having physical security can provide to an organisation.

6. What does Federal Law no. 3 of 1987 refer to?

7. What does Ministerial decision 557 of 2008 refer to?

8. What does Federal Law no. 3 of 2016 refer to?

9. True or False? Private Security Staff are permitted to detain suspects according to the UAE Penal Code.

TRUE / FALSE

10. If you suspect a person is guilty of a crime, but have not witnessed it, can you detain the suspect?

a. Yes, according to the law

b. Yes, ONLY if the suspect consents to being detained

c. No, not permitted at all

11. What are the 4 steps you must follow when making a citizen's arrest?

12. When is it permitted to use force in self-defence according to Ch. 4, Section 1 Article 56 UAE Penal Code?

13. Which article of Wadeema Law states: Give children priority of protection, care, rescue and guidance in cases of emergency, disaster, armed conflict and any crimes committed ?

14. In Abu Dhabi and Northern Emirates, Which directorate is responsible for the regulation of Private Security?

15. In Dubai, which directorate is responsible for the regulation of Private Security?

16. List 5 security license categories available from Abu Dhabi and Dubai

17. What are the 8 personal requirements to apply for a security guard license in Abu Dhabi and Northern Emirates?

18. List the 7 items and equipment that Security staff must carry on them according to Ministerial decision no. 557 of 2008

19. What are the 4 D's of physical security?

20. Give 3 examples of security measures for each of the 4 D's

21. What are the 5 zones of security access?

22. List the 4 public security and safety departments that security staff are most likely to deal with

Module 5
Control room operations

Module 5

Control room operations

Qualification Link

Units

- Nil

Learning outcomes

1. Outline the function of security control rooms
2. Identify laws and regulations related to control room operations
3. Recognise control room technologies and design considerations
4. Apply control room security policy and procedures
5. Summarise roles and tasks within a security control room
6. Identify communication and reporting requirements
7. Identify information security requirements
8. Outline security control room work routines
9. Outline security control room incident response procedures

5.1. Introduction to security control rooms

A security control room is a common way to centralise security resources and operational activities. Security staff will almost certainly interact with a security control room, or work within one themselves.

Figure 39 - Security control room

5.1.1. Purpose and application

A security control room brings together the elements of a security operation, and offers a logical way to coordinate the effects of security systems, personnel and response options. A security control room containing monitoring and control systems can commonly be found in:

- Hotels
- Banks
- Shopping Malls
- Industrial sites
- Airports
- Ports

5.1.2. Laws and regulations governing control room operations

Within the UAE there are several laws and regulations that govern how a security control centre should operate, and the use of CCTV.

Key information

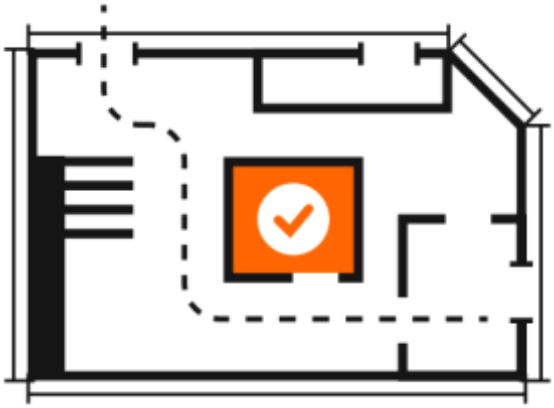
- The Abu Dhabi Monitoring and Control Centre (ADMCC) has published security monitoring standards version 5 as a regulation requirement
- Dubai has Law No. 24 of 2008 regulating security service providers and users, relating to the installation and use of CCTV systems

The ADMCC standards describe the following requirements for CCTV and control rooms:

- Coverage areas for CCTV in various facilities
- Technical requirements of installed equipment
- Design, approval and integration processes
- Security system inspection requirements
- Documentation and logs required

These details are covered in later sections of this module.

5.2. Control room design



The design and construction of a security control room is not the responsibility of Security guards, however understanding the basic elements will help in comprehending the bigger picture of providing security to a site

5.2.1. Technologies and integration

A central security control room provides an opportunity to monitor a variety of technologies and systems. Advances in technology mean that there is a great amount of information that can be viewed easily and quickly through an integrated system.

Key information

Examples of technologies and systems that are found in a security control room:

- CCTV
- Access control and parking management
- Building management systems
- Security alarms and sensors

- **CCTV**
  - Analogue systems
  - Digital I.P cameras
  - Digital Video Recorders
  - Pan, Tilt and Zoom cameras
  - Motion triggered
  - Night vision capable
  - Thermal vision capable
  - Automatic License Plate Recognition (ANPR)

- **Access control systems**
  - Radio Frequency Identification (RFID) badges
  - Keypads
  - Biometric systems
    - Fingerprint
    - Eye Scanner
    - Voice recognition
    - Combination
  - Electro-magnetic locks (remote release)
  - Vehicle barriers & gates (remote release)

- **Building management systems (BMS)**
  - Fire alarm and suppression
  - Elevator controls
    - Emergency intercom
    - Return to ground
  - Heating, venting and cooling (HVAC)
  - Gas sensors and alarms

- **Security alarms and sensors**
  - Perimeter intrusion detection
    - Microwave beam
    - Infrared beam
    - Vibration sensor
  - Door alarms
    - Forced entry
    - Tamper alarm

- Arming and disarming of systems
- System information
  - Location of alarms
  - Time and date
  - Zones breached

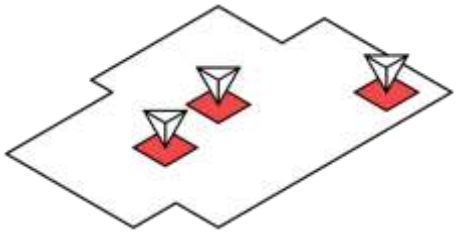
- **Public address systems**
  - Internal communication (intercom)
  - Building speakers
  - Site public address speakers

The number of systems and technologies available are wide ranging, and control room staff will need to become familiar with the specific systems installed at the site or building where they work

Figure 40 - Control room plan

5.2.2. Physical design considerations

The location within a building or site, and the floorplan and layout of the control room are not the responsibility of a security guard, however understanding the design considerations will improve the situational awareness of security staff.



Location

The placement of a control room may impact the performance of security for the site. For example:

- Centrally located
  - more protected by layers of security
  - reduced response times to all areas
- Near site perimeter
  - Ease of access for contractors and essential services
  - More vulnerable to external threats
- Co-located with reception area
  - Suitable for low threat environments
  - Organisational management response may be faster
  - Confidentiality may be compromised due to public access

Room layout

The internal design and placement of desks, screens, doors, windows and other equipment will impact the usability of efficiency of the control room. For example:

- Spacing and location of desks
  - Open plan allows good communication
  - Improve teamwork and collaboration
  - Consider OHS hazards
- Access points
  - Access door positioned away from public zones or reception
  - Should be "air locked" to prevent tail gating through the door
  - May require emergency exit/alternate access points
- CCTV monitoring screens
  - Should be positioned on desks, not on walls
  - Maximum of 3 screens per desk
  - Placed 3 times the distance of the screen diagonal from the user
- Supervisor positioning

    - Located for best situational awareness within the control room
    - Optimised for communication with control room staff
- Windows
    - Depending on security requirements
    - 1-way or 2-way viewing
    - Safety glass – smash resistant
    - Opening or fixed

Each of the design elements may be present in the construction of a security control room, and knowledge of why they are implemented will help Security staff to better understand the overall picture of security at their site.

5.2.3. Security and access control

Controlling who has the ability to enter the control room is of high importance. Critical and sensitive information and activities are exposed within the control room, and only those who need to know should be able to access the room.

Topic focus

Access control can be achieved through a variety of systems and control measures including:

Staff permissions

- Maintained list of who can enter the control room
- Limited to only those who need access
- Regularly updated and monitored

Visitor access control

- Written policy and procedures for allowing visitor access
    - Must have valid reason for visit
    - Must be authorised by manager
- Escorting visitors inside the control room
    - Visitor ID should be issued, to let others know they are authorised to be there
    - A member of the Security staff must be responsible for the visitor
    - Visitors must not be left alone
- Visitor access log completed
- Restrict information on display while visitors are present
    - Black out large CCTV displays
    - Reduce volume of radios
    - Ensure documentation and reports are kept out of view

Physical entry control

- Use electronic security locks
- Access badges issued to authorised staff
- System keeps record of staff entries and exits
- Use a small reception area within the control room to screen people coming in and out
- A biometric access system could also be used as a secondary security layer e.g.
    - Fingerprint reader
    - Eye scanner

It is vitally important that the security of the control room is maintained, as it is the centre of all security operations for a site or even multiple sites.

5.3. Roles and tasks within a control room

There are several defined roles and tasks that will be performed by Security staff while working in a control room. Depending on the organisation and the equipment and systems installed, there might be other roles and duties, but the most basic requirements include:

- Control room supervisor
- Security systems operator
- Communications operator

5.3.1. Security systems operator

The security systems operator may be required to use installed CCTV systems, monitor and respond to alarms and sensors, or control access remotely through gates, doors or other access points. A high level of vigilance, attention to detail and system training is important for a successful security systems operator.

5.3.1.1. CCTV Operator duties

One of the most common tasks within the control room is the operation of a CCTV system. This role is often key in carrying out successful security operations at a site.

Key information

The duties of a CCTV operator are:

- Daily System checks
- Monitoring live video images
- Video patrolling
- Live incident tracking
- Passing information to communications operators
- Retrieval of stored images

Daily system checks

- Camera status 100% functional
- Resolution of video is good
- CCTV operating system working (controllers and software)
- Recording and retrieval system working

A log will be established in the control room for daily system checks to be recorded

Live video monitoring

This is the primary duty of a CCTV operator while working in the control room. It is recommended that a CCTV operator monitors the available video feeds on a 5-minute cycle. The following table describes the expected visual load of a CCTV operator when monitoring live video on the 5-minute cycle:

Area of coverage	Cameras
Perimeter fence with Intruder Detection System and no active security patrols	50
Perimeter fence without Intruder detection system and no active security patrols	15
Crowded public areas with active security staff	15
Crowded public areas without active security staff	5

Table 7 - Live video monitoring load

Video patrolling

The term "Video patrolling" is used to describe the systematic monitoring of certain areas within a site using installed cameras on a designated route or sequence. This technique is used to perform periodic visual inspections, and can include:

- Vulnerable or critical areas
- Remote and low activity areas
- Areas not covered by foot patrols

Video patrolling sequences are normally set by the control room supervisor in cooperation with the security manager. Security staff operating CCTV are expected to follow the video patrolling plans given to them.

Live incident tracking

When a safety or security incident is detected by the CCTV operator, they will continue to track the targets or other elements involved using the CCTV system. This provides the best possible situational awareness for the control room supervisor to form a suitable response plan, and adjust the response if necessary as the situation changes. While live incident tracking, the CCTV operator will:

- Use available video feeds to monitor the location and activity of concerned parties
- Report the locations of concerned parties to the communications operators and supervisor
- Report the actions of concerned parties to the communications operators and supervisor
- Remain vigilant to further safety or security threats during an ongoing incident

Effective communication during live incident tracking is a critical part of successful response to safety and security incidents.

Retrieving recorded images

There will be occasions when the CCTV operator is required to retrieve recorded footage, and the policy and procedure for this activity will be written by the security manager. The CCTV operator must be aware of the policy and procedure, and follow it accurately. Common reasons for retrieving recorded footage include:

- Providing evidence to police
- Internal investigations
- Training activities
- Peer review of security monitoring

If a copy of recorded images is made and issued to police or other departments, an issue report will be completed and logged.

5.3.1.2. CCTV Operator skills and abilities

The skills and abilities required of a CCTV operator are unique, and not all Security staff will fit the nature of the CCTV operator role. There are skills that can be developed through practice and training including:

- Site layout knowledge
- Visual detection techniques
- Behavioural analysis
- Effective team communication

Site layout knowledge

All security staff must have a thorough understanding of the layout of their work site, however CCTV operators need to be able to calculate exact locations using camera locations and video feeds to determine where a safety or security concern is located. Tools available to assist in building this knowledge include:

- Site maps
  - Camera locations
  - Black spots (no coverage)
- Site familiarisation patrols
- Incident response rehearsals

Key information

The ADMCC Chapter 7, Section L requires that all control rooms display a laminated map of each floor with camera locations marked on it. With practice and experience, CCTV operators will instinctively be able to pinpoint locations using the video feeds they are viewing.

It is good practice to mark the camera location map with the actual camera ID, in order to easily identify which camera feed is positioned where on the map. This map can be a detailed floorplan of each level within a building, and additional maps for external cameras fitted at the site.

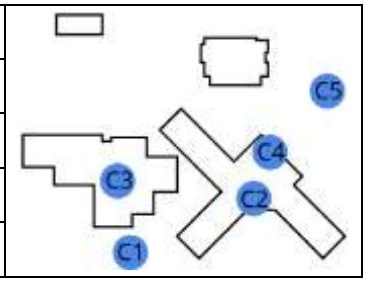
C1-Carpark	
C2-Lobby	
C3-I.T Servers	
C4-Store room	
C5-Deliveries	

Table 8 - CCTV Map example

Understanding where black spots exist in CCTV coverage will guide all security staff when conducting mobile patrols of the area, ensuring that sufficient attention is given to areas that are not monitored. Any black spots should be marked on the CCTV map.

Topic focus

Visual detection techniques

Many CCTV systems have the capability to detect motion, crossing of zones or even heat levels, but humans are able to reason and determine complex scenarios better than any technology can. Detecting a safety or security incident is one of the key skills of a CCTV operator and techniques developed to assist this process include:

- **Change in picture** – what is different about the video feed since last viewing
- **Mental library** – knowing what safety and security threats look like e.g.
  - Materials
  - Equipment
  - Weapons
  - Vehicles
  - People
  - Environmental factors
- **Does it belong** – identifying any element in the picture that does not "fit" within the context of the environment
- **Normal state** – time and experience will show a CCTV operator what is "normal" activity for the site, and the absence of normal will indicate a potential safety or security concern
- **Pattern recognition** – identifying repetitive behaviour can assist in determining if a person or people are behaving in a suspicious or threatening manner

---

A recommended workflow for visual detection can be described as:

Scan – assess the visual picture using the visual detection techniques available

Identify – determine if there is anything that stands out

Focus – Concentrate on target elements, and eliminate distractions. Zoom or clarify the picture if possible

Evaluate – determine if the target elements present a safety or security incident

Decide – escalate the incident if required, or continue to monitor

Behavioural analysis

Understanding human behaviour can assist a CCTV operator in determining if there is suspicious or threatening behaviour. Behaviour analysis is the process of reading non-verbal communications. This typically consists of:

- Personal space
- Posture
- Eye contact
- Gestures
- Threat profiling
- Hostile surveillance

Personal space

Identifying personal space is a strong indicator of relationships between people. Normally, close personal space is reserved for spouses or family members, while distant spacing is used for unknown members of the public. The following is a table of established zones of personal space:

Zone	Distance	Relationship
Close intimate	< 15cm	Spouse and family
Intimate	15-45cm	
Personal	46cm-1.2m	Business or casual
Social	1.2 – 3.6m	Unfamiliar people
Public	3.6m +	

Table 9 - Personal space zones

Posture

A persons' posture can be read to interpret their intentions. Posture can also be used to conceal carried items or weapons. Examples of posture interpretation can include:

Interpretation	Posture
Defensive	Hands held up
	Arms folded
	Shaking head
	Body turned away
Aggressive	Leaning forward
	One leg forward
	Tense
Nervous	Fidgeting
	Pulling at hair
	Rapid movement
Suspicious	Rigid walk
	Rigid torso when turning
	Bulges in clothing
	Favouring a particular foot

Table 10 - Posture examples

Eye contact

Depending on the resolution and capability of the CCTV system, it may be possible to analyse eye contact between people. Knowledge and interpretation of eye contact may assist the CCTV operator in determining the relationships, intensions or threats to safety and security. Examples of non-verbal communication through eye contact may include:

- Intimidation
- Cooperation
- Personal interest or surveillance

Normally, eye contact between strangers is very brief. Longer eye contact is held between people who know each other or are communicating with one another.

Gestures

Physical gestures are often a clear indicator of behavioural intent. Things such as pointing, waving, and clenched or waving fists signal the intent of that person. A CCV operator can use the social and cultural context to interpret gestures and determine if the person is a potential threat to safety or security.

Threat profiling

A useful tool when analysing behaviours is to establish a profile of various potential threats identified for a site or organisation. This can include describing for each threat:

- Typical clothing and accessories
- Physical attributes
    - Gender
    - Age
    - Build
    - Ethnicity
    - Cultural identifiers
        - Religion

        - Markings
- Interpersonal contact
    - Cultural context of personal space
    - Family groups

Building a profile for identified threats, and then comparing attributes of a monitored target can help in evaluating if a safety or security incident is presented, and determining the appropriate actions.

Hostile surveillance

Almost always, before a deliberate security breach occurs the person or people involved will carry out some form of surveillance. A CCTV operator must remain vigilant to the act of hostile surveillance, and doing so can assist in preventing security breaches. Examples of suspicious activity that may indicate surveillance includes:

- Repeated passing of the same vehicle
- Filming or taking photos of security areas
- Drawing or note taking
- Extended waiting around for no apparent reason
- Asking questions about security systems
- Repeated false alarm activations
- False delivery of packages
- Persons found in "off limits" areas, particularly areas allowing access to critical systems e.g. heating, venting, cooling or electrical systems

5.3.2. Communications operator

The communications operator role is another major activity within the control room and can be divided into two sub-roles:

- Radio operator
- Communications logger

These two tasks are vital to a successful security operation. Detailed information on the communications process is given in a later section.

5.3.2.1. Radio operator

The radio operator will use radio communication equipment to relay information across the security team.

Key information

The primary duties of a radio operator include:

- Equipment inspection and testing
- Message sending
- Message receiving
- Troubleshooting
- Frequency management

Equipment inspection and testing

The radio operator will check that all radio equipment and accessories are available, and working correctly before starting duty. The Inspection process will include:

- 100% equipment accounting
- Battery levels full + spares available
- Belt clips, antenna and earpieces in good condition
- Transmit and receive working correctly

Sending and receiving messages

The radio operator will send and receive messages using the established radio procedures. The radio operator will also escalate incidents to the control room supervisor, enabling incident response decisions to be made. This procedure is described in detail in the communications and reporting section

Troubleshooting

If a radio or its network fails, the radio operator must carry out user level troubleshooting and attempt to restore communications. This process is described in the following communication procedures section.

Frequency management

More complex security operations may utilise several frequencies for communication, with different sectors or staff using each frequency. The radio operator is the central point of communication and must manage communications passing through multiple channels, and be able to select and switch channels to communicate with the appropriate people.

5.3.2.2. Communications logger

The communications logger is responsible for recording all communication passing through the control centre. The logger will:

- Log security issues when they occur
- Log alarm activations and cancellations and reasons why they occurred
- Log decisions made by supervisors and managers
- Log potential security issues
- Prepare daily reports for the control room supervisor

Best practice for logging is to keep 2 logs, 1 for daily occurrences, and a second log for supervisor decisions. An electronic version can be kept in addition to a written log to enable better data analysis and retrieval.

Key information

- When completing communications log entries, rough notes can be kept and then transferred neatly into the written log and updated in the electronic log
- Communications logs may be referred to during legal investigations – accuracy is essential.

Topic focus

Logging communication

A best practice for the process of logging communications within a control room can be summarised as follows:

- Handwriting is clear and accurate
- Entries written in black ink
- When coming on to logging duty, the date and signature of incoming logger should be recorded
- Entries in chronological order with the time of each entry recorded in 24hr format
- Entries numbered in sequence
- Record only facts, not assumptions
- Clearly show errors by drawing a single line through the error, with correction made and initialled
- No entries are to be erased
- No blank spaces or pages are permitted
- No pages can be removed or added
- When changing over duty, the log should be ruled under the last entry, and signed by the outgoing logger

#	Date / Time	From	To	Message
25	1430	Lobby	CR	Visitor escort
Mohammed Al Ali				

18-12-18		Saif Al Zaabi		
26	1445	Gate	CR	Rotating post
27	1515	Gate	CR	Delivery truck

Table 11 - Example communications log

5.3.3. Control room supervisor

Security staff working in the control room will not be required to supervise the operations, however understanding the role of the control room supervisor will assist others in the control room to work closely with and support the supervisor. The control room supervisor will be responsible for:

- Day to day functions of the control room
- Deploying reserve security staff to incidents
- Formulating and directing response to safety and security incidents
- Escalating critical incidents to the security manager
- Preparing reports for the security manager

Critical incidents may be escalated to a separate incident management team, with their own incident room. This will depend on the type of organisation, and the anticipated risks and threats.

5.4. Communications and reporting

Communication is one of the most important elements in a successful security operation, and having a clear communication plan and process will assist all members of the team to work together in cooperation.

5.4.1. Chains of command

A clearly defined chain of command will reduce confusion and ensure that the passage of information across the team flows in a coordinated manner. A typical chain of command would look like this:

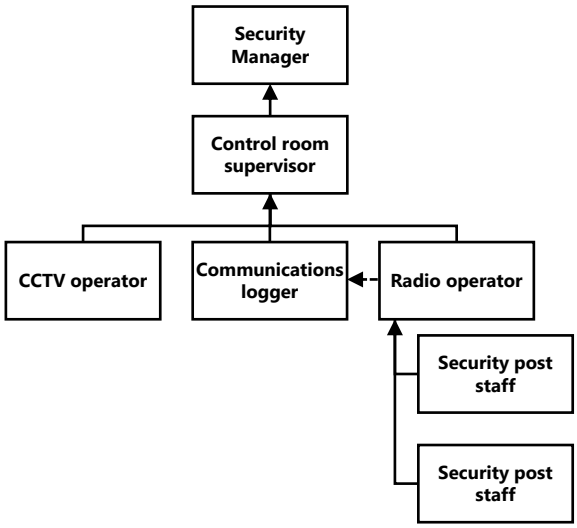


Figure 41 - Reporting chain example

5.4.2. Communication pathways

An established communication pathway will be required when using radios for communication because if there are many staff using the radio, there is potential for confusion and loss of information. This is normally referred to as a radio network. A radio network is made up of:

- Call signs
- Frequencies
- Equipment
    - Handheld radios
    - Base station radio

Key information

Call signs

A call sign is a unique name used to identify a person or position of duty within the security team. There can only be one of each callsign on a radio network. Examples of this are:

- Control room
- Escort 1
- Escort 2
- Patrol 1
- Patrol 2
- Checkpoint 1
- Checkpoint 2

The actual names of call signs used will depend on the site or organisation.

Frequencies

This refers to the broadcasting frequency of the radios used. A simple method of referring to frequencies is by channel. A radio channel can be programmed to a set frequency, and that channel then allocated to a particular team or purpose. Channel allocation could look like this:

Frequency	Channel	Group
450Mhz	1	Entry control Point
525Mhz	2	Mobile patrol
650Mhz	3	Reception security

The purpose of allocating channels to sub groups within a security operation is to reduce the confusion and the amount of traffic coming across the radio at each post or location.

Radio network diagrams

To make the communication pathways clear, a radio network diagram can be drawn that will describe the call signs, channels, and reporting lines within a security operation. An example of a radio network diagram follows:

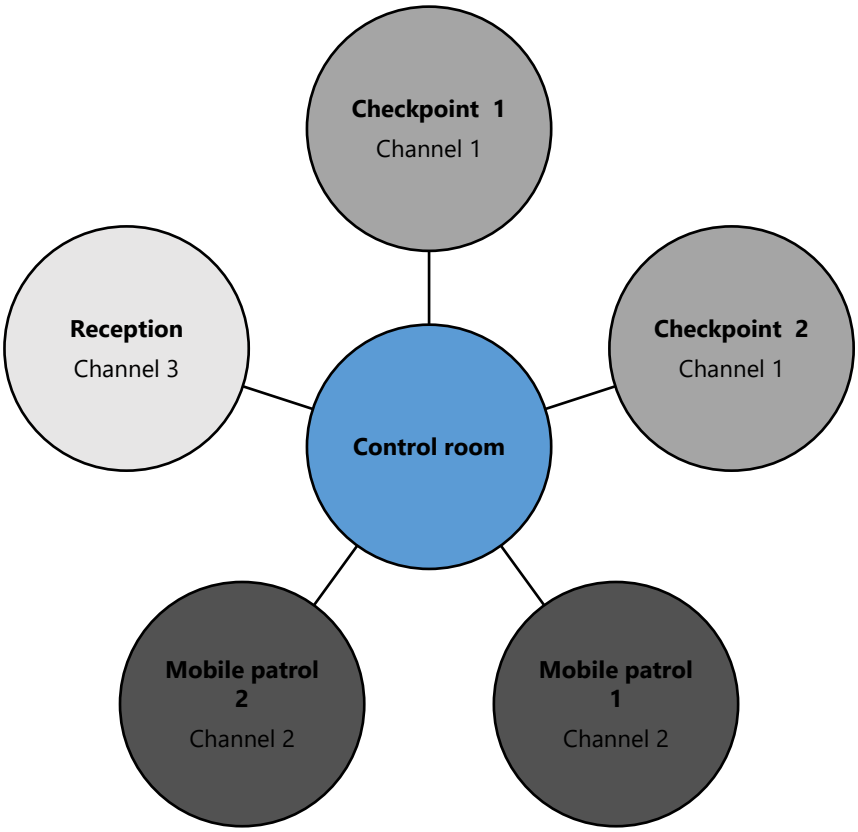


Figure 42 - Example radio network diagram

5.4.3. Radio communication equipment

A radio is one of the most essential pieces of equipment available to security staff. Understanding the radio types available, the parts and components, and how to safely handle the radio is vital to a successful security operation.

Radio types

There are many manufacturers and brands of radio, however most will be designed as one of the following:

- Hand held
- Vehicle mounted
- Base station

Most mobile security staff will carry a hand held radio, while fixed duty locations may use a base station.

Radio parts

Hand held radios will usually have:

- Radio body
    - On/Off switch
    - Channel selector
    - Press to talk button
- Battery
- Charging cable / base
- Antennae
- Belt clip
- Earpiece
- External microphone

Figure 43 - Example hand held radio

Vehicle mounted radios are installed in the dashboard of a car or patrol vehicle, and can offer extended transmitting ranges. The radio will consist of:

- Radio body
- Internal speaker
- External microphone

Figure 44 - Vehicle mount radio

A base station radio is normally used in a control centre or other fixed location. The base station radio will consist of:

- Radio body
- External speaker
- Antennae outputs
- Channel switches

Figure 45 - Base station radio

5.4.4. Communication procedures

A standard method for using a radio to communicate is essential for efficient communication and passage of information. There are globally established standards for radio communication that cover:

- Forming radio messages
- Radio network etiquette
- Use of the phonetic alphabet

Radio messages

To send a message over the radio network, specific information is required. The simplest way to describe this is as follows:

Topic focus

Starting a radio call					
Information:	Receiving call sign	Identify	Transmitting call sign	Message	End of transmission
Say:	*Patrol 1*	*This is*	*Control Room*	-	*Over*

Sending a radio message					
Information:	Receiving call sign	Identify	Transmitting call sign	Message	End of transmission
Say:	*Patrol 1*	*This is*	*Control Room*	***Send current location***	*Over*

Ending a radio message					
Information:	Receiving call sign	Identify	Transmitting call sign	Message	End of transmission
Say:	*Patrol 1*	*This is*	*Control Room*	*Roger*	***Out***

Continuing the conversation

It is acceptable once the conversation has been established, to stop saying your own call sign at the start of each transmission, and instead only announce your call sign when closing the radio call. For example:

- "Patrol 1, this is control room, over"
- "Control room, this is Patrol 1, over"
- "Patrol 1, send current location, over"
- "Control room, Location A1, over"
- "Patrol 1, this is control room, roger, out"

Key information

To achieve a clearly transmitted message, the following points should be remembered:

- **Rhythm** – Speak in a predictable rhythm
- **Speed** – Speak slowly enough to be clearly understood
- **Volume** – Do not shout or whisper, a normal conversational volume is required
- **Pitch** – A very low pitched voice is difficult to understand when transmitted by radio

Radio etiquette

It is good practice to allow an ongoing radio conversation to finish, rather than interrupting. The only time when it is acceptable to interrupt, is when there is a safety or security issue that takes priority.

Lost communications procedure

If there is a loss of radio communications the following steps are to be taken in order:

- Check all connections on the radio e.g.
  - Antenna
  - External Microphone
  - Battery fit
- Power of
- Replace the battery
- Power on
- Move to another location and try again
- Revert to alternate channel
- Switch to alternate method of communication e.g. mobile phone
- Return to control room

Alternative communications plan

It is important that a plan is established should communications fail using the primary method. Normally this would include:

- Assigning alternate radio channels as backup
- Landline phones at specific locations
- Mobile phone
- Using a runner to relay messages

Black spot mapping

The nature of radio communications means that in certain environments or with particular radio frequencies, there will be areas where clear communications are impossible. It is important that a security team are aware of areas within their site that prohibit clear radio communication. A best practice method is to map the "black spots" of radio coverage. A map can then be kept in the control room, and this should be updated when:

- New frequencies are used
- New radio equipment is purchased
- Security teams first occupy a site
- After any construction or modifications at the site

5.4.5. Reportable information

Understanding what type of information should be reported will make the security operation efficient and responsive. Security staff must be aware of the information that they are required to pass up the reporting chain, and each site or organisation will have different requirements set out in standard operating procedures (SOPs). Common examples of reportable information include:

- Health and safety concerns
- Potential security issues
- False alarm activations
- Actual security incidents
- Equipment loss or damage
- Customer complaints
- Internal conflicts

Each type of reportable information will have an associated reporting format. The standard formats used will be covered in a later section.

Key information

A daily summary report will be prepared by the site or organisational security manager for submission to the national security operations room. The normal flow of information going into this report would be:

1. Security staff notebook
   ↓
2. Incident reports
   ↓
3. Control room daily report
   ↓
4. Security manager report
   ↓
5. Submitted to National Security Operations Centre

The specific communication and reporting requirements will be different for each site or organisation, but security staff should be familiar with what to look for when taking up duty at a new location. The information contained in this section will serve as a starting point, with further details coming from site or organisational SOPs.

5.5. Information security

Aside from the physical security measures applied to a control room, security staff must be aware of information security threats, risks and consequences of failing to follow good information security practices. Best practice for information security standards can be found in the Abu Dhabi Systems and Information Centre manual of Information Security Standards.

Figure 46 - Information security

Key definitions

- **Information security** – being protected against the unauthorised use of information, including electronic data, and the measures taken to achieve this.

5.5.1. Information security threats

Topic focus

Threats to the security of information can compromise not just a security operation, but also larger parts of an organisation or business including:

- Trade secrets
- Personal data
- Financial records

Understanding how information could be accessed by unauthorised people can help security staff to safeguard against it. Examples of methods to access sensitive information include:

Physical access

- Visual exposure
  - Computer screens
  - Desks
  - Notice boards
  - Printer tray
- Theft
  - Opportunity – unsecured documents
  - Forced entry
- Copying
- Photography and recording

Digital access

- Wrong recipient on emails
- Unsecured computer networks
- Social media

5.5.2. Storage and destruction of information

Organisations will employ policy and procedure to guide how information should be stored, and the requirements for destroying security classified information. Characteristics of information that requires secure storage include:

- Exposes vulnerabilities of an organisation, premises or services
- Can lead to financial loss
- Can embarrass an individual or organisation

- Can compromise personal data

Any information that could reveal this type of detail must be securely stored.

Figure 47 - Destroyed physical information

5.5.2.1. Information security policy

Organisational management will implement information security policies describing the processes and procedures for handling confidential or sensitive information. The policy will include guidance on:

- **Classifying information**
  - Classified and marked according to the impact of its disclosure
- **Access privileges**
  - Who is permitted to access and view the information
  - How to verify the access permission e.g. Lists of staff verified by I.D
  - Access logging requirements e.g. a record kept of who has accessed the security classified information
- **Storage requirements**
  - How each classification of information must be stored
- **Destruction requirements**
  - How each classification of information can be disposed of
  - Documentation of disposal e.g. a record kept of what information was destroyed and when
  - Who can authorise the disposal of classified information e.g. Line manager, security manager, board members etc.

Figure 48 - Lockable filing cabinet

5.5.2.2. Methods of physical information storage

Key information

Security classified information can be kept securely using a variety of methods, and depending on the impact of disclosure higher levels of security may be employed. Examples could include:

- Kept in a folder while out of secure storage
- Locked filing cabinet
- A safe
- Access controlled archive room

A combination of these measures could be utilised e.g. kept inside a locked filing cabinet, inside an access controlled archive room.

5.5.2.3. Methods of physical information destruction

There are a variety of methods available for destroying security classified information that is no longer required to be kept. Depending on the level of classification, and organisational policy, options for destroying can include:

- **Burning**
  - Controlled burn of documents and removal of ashes
- **Pulping**
  - Mixing with water and reduced to pulp
- **Shredding**
  - Documents cut into fine strips by machine, the width of the strips may be specified according to information security policies
- **Cross-shredding**

- Documents passed through an industrial shredder at 90 degree angles to produce fine squares

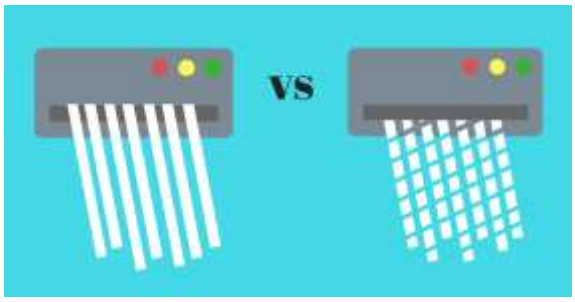


Figure 49 - Strip cut vs Cross cut shredding

5.5.2.4. Digital information storage

Security classified information may be kept in a digital format and the storage arrangements must also be considered. The type of information and its impact of disclosure will determine the security storage methods chosen, however some options may include:

- Computer based storage
  - Password protected files
  - Password protected computers
  - Cloud based storage
  - Intranet (internal network) storage
  - Printing restrictions
- External media storage
  - Encrypted USB Flash drive
  - Racked mass storage drives
  - CD/DVD

These options have strengths and weaknesses, and these should be evaluated before committing to a particular method for storing security sensitive information.

CD/DVD

Secure network

Flash drive

Cloud storage

Table 12 - Digital information storage options

Specific consideration should be given to the recording and storage of security camera video images. There are currently 2 common methods for recording and storing these images:

- Digital Video Recorder - DVR
- Network Video Recorder - NVR

A DVR system will record the camera feeds onto a mass storage drive located locally within the security control room.

The strengths of a DVR system include:

- Physical access required to the system to retrieve or remove footage

Weaknesses include:

- Inability to share recorded footage across remote locations
- May be corrupted or damaged by local disaster

The strengths of an NVR system include:

- Ability to record images over an internet network
- Can scale the size of the CCTV network easily
- Recorded images can be accessed remotely

Weaknesses include:

- Vulnerable to unauthorised remote access(Hacking)
- Network outages may result in lost recording time

5.5.2.5. Digital information destruction

A variety of methods are available to securely dispose of digital information. The method used by an organisation will depend on the sensitivity of the information, cost and regulatory requirements. Some examples of destruction methods include:

- **Granulation**
  - The process of grinding down physical storage media into fine particles
- **Degaussing**
  - The process of removing magnetic information from media storage devices
  - Commonly used to securely remove information from:
    - Storage tapes
    - Hard drives

Media storage crushing machine

Drive and tape degaussing machine

Table 13 - Digital information destruction machines

The most common reason for destroying digital media storage, is when a storage device is being retired, or no longer needed. The risk of information that remains on the device being exposed is too great, and the information must be permanently destroyed.

5.5.3. Visibility of sensitive information

Topic focus

Security staff must remain aware of the visibility of any information that is not classified in such a way that it is permanently secured, but still presents a risk should members of the public or other groups be able to view. Typical areas to monitor for sensitive information include:

- Noticeboards
- Desk space
- Computer monitors
- Video monitors

All security staff can monitor what information is on display, and take action to remove from visible display if required.

Figure 50 - Computer screen privacy hood

5.5.4. Release of recorded images

Key information

If there is any request to receive copies of recorded images captured by the control room, an authorisation form must be completed to document the release to a third party. The Abu Dhabi Security Monitoring Standards provides a form reference MCC/SMS/ICIL that can be used to record the details. The information required when issuing a copy of recorded images includes:

- Date and time of image capture
- CCTV operator name
- Camera I.D
- Incident record number
- Receiving officer name
- Receiving officer contact details
- Receiving officer signature
- Date of return or destruction
- Security manager signature

An example of this document can be found at the end of this module.

A strict policy must be followed when consenting to release recorded images, as the confidentiality of others will be breached. The most common occasion for releasing images will be to provide the police with evidence after an incident has occurred.

5.5.5. I.T and Cyber security

Although I.T security is a specialised field, Security staff must be familiar with the basic concepts in order to maintain vigilance towards the threat of compromise through I.T systems.

Basic precautions to consider include:

- Allow computer systems and software to run updates
- Ensure virus scanning software is installed and running
- Use strong passwords for online systems including a combination of letters, numbers and special characters
- Do not open emails received from suspicious senders – report to I.T department
- Restrict physical access to computer workstations
- Report any unusual behaviour by computer systems e.g.
    - Apparent loss of control
    - Flickering or erratic screen

- Pop-up windows

Figure 51 - Virus scanning tools

More advanced precautions against cyber threats are available, and some highly sensitive sites may utilise a technique known as "air-gapping" their data storage. This means that the computer systems that contain the classified information are not physically connected to any networks or internet, removing the opportunity for remote intrusion and theft.

5.6. Daily routine and procedure

Daily routine within the control room will be described within the post duty instructions, and a typical control room routine will involve shift hand over, specific duty rotation, rest breaks, and the completion and filing of reports.

Figure 52 - Shift work

5.6.1. Documentation and reports

Key information

The communications logger working within a control room will be responsible for the completion and filing of various documentation and reports including:

- Daily incident summaries to PSBD operations
- Maintaining the visitors log
- CCTV Incident log
- CCTV Maintenance / Fault Log
- CCTV Daily system check log
- CCTV Viewing Log
- CCTV Image copy release log

Example of these logs and reports are found at the end of this module.

5.6.2. Fatigue management

The demands of working in a control room will require long periods of concentration and attention to detail. In order to effectively work in this environment, fatigue must be planned for and managed. The approach for managing fatigue within a control room fill be the responsibility of the Security manager, and will include:

- **Shift timings**
  - Dependant on available staff numbers
  - Depend on site requirements
  - 2 x 12 hour shifts are common; however, 3 x 8 hour shifts are ideal e.g.
    - 0600-1400
    - 1400-2200
    - 2200-0600
  - Oncoming shifts will need time to hand over, so overlap is planned for
- **Shift rotations**
  - Staff will be rotated from early shifts to late shifts through a cycle e.g.

Day 1	0600-1400
Day 2	0600-1400
Day 3	1400-2200
Day 4	1400-2200
Day 5	2200-0600
Day 6	2200-0600
Day 7	**Off duty**

  - This will reduce the negative effects of shift working
- **Task rotations**
  - Frequent rotation of control room tasks will ensure staff remain highly vigilant

- Task rotation every 30 minutes is good practice e.g.

CCTV operator	0600-0630
Radio operator	0630-0700
Communications	0700-0730
Break	0730-0745

- Staff numbers will impact rotation

- **Planned breaks**
  - Control room Security staff must be able to recharge energy and be able to escape the intensity of control room work
  - A separate break area should be allocated, outside of the control room
  - Regular, short breaks can be used with a longer break taken periodically
  - Security managers will design an optimal shift break pattern

Figure 53 - Shift fatigue

5.6.3. Shift hand over

The handing over of duty to an incoming team is one of the most critical parts of a security operation. The continuity of a quality security service depends on a smooth and accurate hand over of responsibility. The primary benefits of a well organised shift hand over are:

- Increased situational awareness for incoming team
- Management of ongoing issues
- Continuity of security operations

Key information

It is vital that the shift hand over is done in an overlapping method, known as relief in place. The incoming Security staff will arrive at individual posts to relieve the outgoing staff, achieving 100% security coverage at all times.

It is good practice for security shift supervisors to give a collective briefing to incoming staff, alerting them to any significant activities that have been carried out by the outgoing shift, and any planned work that needs to be completed during the next shift.

Topic focus

A shift hand over checklist can help staff to ensure that the hand over process is completed accurately and smoothly. Information to cover includes:

- Resolved incidents
- Ongoing incidents
- Changes to site staff / contact information
- Technical or site issues
- Unusual occurrences
- Numbers and position of duty security staff
- Signing over of duty equipment

Using this approach will ensure that all staff are aware of what is happening within their site, and are able to recognise potential problems before they occur.

Figure 54 - Shift handover checklist

5.7. Incident response procedure

Staff working within a control room will need to be familiar with the steps to be taken should an incident occur. The site Security manager will provide standard operating procedures to the staff, and these procedures will include:

- Escalation procedure
- Who is in control
- Staff who are expected to respond
- Controlling movement of staff

- Evacuation procedure if required

- **Escalation procedure**

Normal procedure for incidents requiring escalation will be to notify the control room supervisor, who will then escalate to the Security manager.

- **Incident control**

Any active incident will be controlled by the control room supervisor

- **Expected response staff**

Situation dependant, however stand by security personnel, fire warden, first aider, facilities management and I.T support may be required to respond

- **Controlling staff movement**

During an ongoing incident, the movement of responding staff must be controlled in order to reduce the risk of further complicating an incident. Safety and security will be considered by the control room supervisor, and instructions given through the control room radio operator to responding staff regarding:

- Locations to move to
- Routes to take
- Time to move
- Precautions to take based on monitoring of the situation
- Other responding staff or external agencies expected to be in contact with

- **Evacuation procedures**

All staff must be aware of the evacuation procedures specific to the place of duty, and what events will trigger an evacuation. Such events may include:

- Uncontrolled fire
- Hazardous material spill
- Gas leak

These details will be contained within site SOPs

5.7.1. Actions for security incident

All sites and organisations will have unique actions required to be followed, however a general guide for actions to when responding to security incidents can be useful for Security staff to use as the base of security operations.

Topic focus

5.7.1.1. Alarm activation

If an alarm sounds or indicates in the security control room:

- Identify the source of the alarm e.g. Fire, gas leak, intrusion detection, camera outage etc.
- Identify the location of the alarm
- Communicate the alarm status to nearest security staff
- Instruct nearest security staff to investigate and confirm the situation
- Carry out incident response procedure based on confirmation of incident
- Document and record according to SOPs

5.7.1.2. Perimeter breach

If a site perimeter breach is confirmed:

- Call the police
- Monitor the area through CCTV or security personnel to locate the intruder(s)
- Identify if any theft, damage or other operational impact has occurred
- If intruders are located, detain in accordance with the legal requirements
- Document and record according to SOPs

Figure 55 - Perimeter breach

5.7.1.3. Theft

If a theft is identified or reported:

- Record the date, time and location
- Call the police
- Use available monitoring systems to review images of the area
- Instruct Security staff to take any witness statements
- Request Security staff preserve any evidence and the suspected crime scene
- Document and record according to SOPs

5.7.1.4. Bomb threat

If a bomb threat is received in the security control room:

- Signal to others that a bomb threat is in progress according to SOPs (the control room supervisor will arrange for the police to be called)
- Remain calm and be courteous to the caller
- Don't interrupt the caller
- Try to keep the caller talking in order to determine as much information about them as possible
- Complete the bomb threat checklist
- Evacuate the threatened area according to SOPs

Figure 56 - Telephone bomb threat

5.7.2. Actions for safety incident

Safety incidents will be responded to by Security staff, and the control room operators will coordinate this response. If a health or safety incident is identified:

- Instruct attending Security staff to make the area safe e.g. control access to the area
- Request incident details
- Determine the required department to rectify the issue
- Coordinate the response of maintenance or facilities management
- Process the attending security staff incident report
- Document and record according to SOPs

Key information

If a health and safety issue has been identified that poses an immediate risk to site personnel, do not allow the issue to go uncontrolled. Maintain a Security presence at the location until the issue has been resolved, or handed over to the relevant department.

5.7.3. Actions for equipment failure

Equipment failure can severely impact the success of a security operation. The type of equipment and its necessity will dictate the actions to be taken, and could be categorised as follows:

Critical

- Life support systems i.e.
    - Ventilation of toxic gases
    - Water treatment
    - Fire detection and suppression

Should any life support systems fail, serious consideration must be given to evacuating the building or site in order to reduce the risk of harm to personnel.

Security Operations

- CCTV Cameras
- Intrusion sensors
- Communications equipment
- Barriers and gates
- Searching equipment

Topic focus

Loss of capability through equipment failure may result in a compromised security operation. If any of these types of equipment fail, control room operators should:

- Deploy security staff to the failure location
- Initiate an urgent maintenance request
- Deploy available back up equipment
- Document and record in accordance with SOPs

Security supervisors will assess the risk and severity of the equipment loss, and may initiate a full or partial lockdown of certain sites.

Non-critical operations

- PPE
- Lights, air conditioning or heating

The failure of equipment related to the comfort of staff, or general facilities will need reporting to maintenance and the situation documented and recorded in accordance with SOPs

5.7.4. Actions for lost communications

As the centre of the security operation, a loss of communications is a serious problem for the control room. Depending on the actual communications technology used, a standard action to be taken could include:

- Switch radios to alternate channel
- Use secondary communications device e.g.
    - Mobile phone
    - Land line phones
    - Intercom system
- Send resting control room staff to bring replacement radios to remote staff
- Request technical support
- Maintain critical communication pathways via foot messenger

5.7.5. Actions for power failure

Should a site or part of a site experience a power failure:

- Identify any critical systems that may be blacked out e.g.
    - CCTV coverage
    - Intrusion alarms
    - Access control systems
- Direct remote staff to the affected area to attempt re-setting of local power at the switch panel
- Deploy Security staff to cover critical areas affected by power loss
- Call facilities management for urgent maintenance
- Escalate to municipal utilities service if required
- If a health and safety risk is presented, coordinate the evacuation of non-essential staff from the affected area

Figure 57 - Power failure on site

Key definitions

SOPs – Standard Operating Procedures

Control room – Central operations room of a site security service

CCTV – Closed Circuit Television

BMS – Building Management System

ADMCC – Abu Dhabi Monitoring and Control Centre

Target – Suspect, or person of interest

Monitoring – Continuous viewing of a situation, area or target

DVR – Digital Video Recorder

NVR – Network Video Recorder

Further research

- Abu Dhabi Monitoring and Control Centre Standards v5.0
- Dubai Law No. 24 of 2008

Example control room documentation

PSBD daily incident report

Company Daily Incident Report					
Day		**Date**		**Time**	
Emirate			**Location**		

Phone number	
Reporting Security Staff Name	
Nationality	
Company Name	
Location	
Incident/Accident type	
Response procedure taken	
Company operations staff Name	
Company operations incident summary	
Received at PSBD Operations by	
Rank	
Name	
Date	
Signature	

Control room visitor log

Date	Arrival time	Departure time	Surname	Initial	Organisation	Position	Signature	Signed in by

CCTV Incident log

CCTV Incident Log					
Date		**Time**		**Location**	
Incident type					
Recording number			**Live incident recording Y/N**		
Reporting person name				**Employer**	
Description of incident					
Response to incident					
Police requested at time				**Time of police arrival**	
Name of attending police				**Police number**	
Medical requested at time				**Medical arrival**	
Name of attending medics					
Name of control room supervisor				**Signature**	

CCTV Maintenance / Fault report log

CCTV Maintenance / Fault report log					
Date		**Time**		**Engineer**	
Reason	☐ **Regular maintenance**		☐ **Call out**		
Maintenance details					
Outcome					

Viewing log for recorded CCTV

Viewing date	Viewing time	Camera ID	Operator name	Persons viewing	Organisational Details	Reason for viewing	Outcome if any

Issued copy of CCTV images log

Issued copy of CCTV images log			
Reason for provision	**☐ Legal proceedings**	**☐ Subject access**	**☐ Other**
Date of creation	**Time of creation**	**CCTV Operator**	**Camera ID**

Incident number	
Police or Third party name	
Contact details	
Signature of third party	
Date of destruction or return	
Security Manager signature	

Daily CCTV system check log

Date	Time	Operator	Date/Time stamp checked	Camera and recording quality checked

Module 5 Revision

Revision questions

1. List the 3 main roles within a Security Control room?

2. Identify 2 laws and regulations governing the operation of security control rooms in the UAE?

3. List 5 examples of technologies that could be integrated within a control room

4. All visitors to a control room must be logged and escorted – True or False

5. List 3 tasks of a CCTV operator

6. List 2 tasks of a communications logger

7. List 3 tasks of a radio operator

8. Outline the chain of command and reporting within a standard security control room

9. Identify 3 radio accessories used in security operations

10. Identify 4 examples of reportable information

11. List 3 ways to destroy physical documents

12. List 2 methods of secure document storage

13. List 3 potential I.T security threats

14. List 3 locations that sensitive information may be visible in the workplace

15. Identify 5 pieces of information that could be included in a shift handover checklist

16. Outline the procedure for handling a telephone bomb threat

17. Name the procedure for overlapping security shifts during hand over

18. Name the document that needs to be completed when issuing recorded images to police or a third party

Module 6
Patrolling

Module 6

Patrolling

Qualification Link

Units

- SEC03004NU18-Conduct site security patrols
- SEC03003NU18-Use security search methods and equipment

Learning outcomes

1. Interpret site security plans and prepare for security patrols
2. Conduct security patrols
3. Carry out inspection of key security areas
4. Search structures
5. Use standard formats to document patrol activity

Key definitions

Security Patrol – Travelling a route or path with the aim of enhancing the safety and security of a site or area

Dismounted – Moving by foot

Mounted – Moving by any vehicle type

Patrol report – Standard report documenting security patrol activities

Key information

The 4 P's of patrolling

Protection of life:

from dangerous / hazardous situations, assault, or emergency situations

Protection of property and premises

Protecting property from theft, fire, criminal damage, or defacement.

Prevention of loss and waste

Loss by theft, breach of confidentiality, or abuse of client's property, such as unauthorised use of computers, telephones or other equipment.

Preventing and deterring crime

Theft, breach of peace, criminal damage, public order offences

6.1. Aims and methods of patrolling

One of the primary duties of Security staff are to conduct periodic patrols of the site or area for which they are responsible. There are various aims when conducting patrols, and methods by which the patrol is carried out.

6.1.1. Security patrol aims

The primary aims of security patrolling will vary slightly depending on the organisation, however the following can be referred to as a foundation for why Security staff conduct patrols:

Further aims can be identified as:

- Increased situational awareness
- Providing an overt physical security presence
- Reducing response time to critical areas
- Inspecting the status of security measures
- Deterring criminal activity
- Increasing alertness of Security staff
- Providing customer service

6.1.2. Methods of patrolling

There are several methods that Security staff can use to conduct patrols, each with its own benefit and weakness. The most common methods include:

Walking patrol

This form of patrolling is the most common, and is utilised in most organisations.

Benefits include:

- Enhanced situational awareness
- Can utilise human senses
- Ability to inspect closer detail
- Interaction with staff, and members of the public

Weaknesses include:

- Time required to cover larger areas
- Physically exhausting
- Environmental exposure

Vehicle patrol

Vehicle patrols could take many forms including:

- Car
- Golf Buggy
- Cycle
- Segway

Benefits include:

- Ability to patrol a large area or perimeter
- Can be fitted with supporting technologies such as:
    - Radio
    - GPS tracker
    - High powered lighting
- Can keep Security staff protected from the environment during patrols

Weaknesses include:

- High profile may alert criminals to an approaching patrol
- Removes the ability to use some of the human senses
- Can be expensive to maintain and operate

Remote technology patrol

Technologies can be used to survey areas in a form of "Remote Patrolling". Examples of this include:

- CCTV Cameras
- Drones

6.2. Site plans and patrol routes

It is essential that Security staff tasked with performing security patrols understand the layout of their work site, and established patrolling routes.

Key information

Site security plans, patrol maps and patrol instructions can be found in a sites Security Control Room

6.2.1. Site layout and security systems

Security supervisors and managers are responsible for maintaining site plans with critical systems, key locations and security measures marked. Security staff can refer to these maps to aid in the familiarisation of the site, and where the relevant utilities, systems and infrastructure is located.

Key information

When reading a site plan map look for the following details:

- **Version** – always use the latest
- **Legend** – ensure the symbols indicating critical systems, locations and security measures are understood
- **Scale** – identify the size of the area to be patrolled
- **Orientation** – make sure the site plan layout is understood (Normally oriented to north)
- **Perimeter** – identify the boundaries of the site
- **Zones** – identify the boundaries of any zones within the site plan

Some site plans may be supplemented with satellite imagery, digital renderings, or even scale models that allow for an enhanced understanding of the site.

6.2.2. Crime prevention strategies

Site security plans may include specific strategies to prevent and deter crime. The patrolling staff should confirm these strategies and ensure that measures within the site are in support. Specific strategies could include:

- Increasing the risk for criminals
    - Chance of detection
    - Exposure to public
    - Enforcement of laws
- Reducing reward for criminals
    - E.g. Compartmentalising valuables
- Increasing difficulty in committing crime
    - Deny access
    - Security depth e.g. 4 D's
- Reducing temptation for criminal activity
    - Removing valuable items from view
    - Constant vigilance of security
    - Warning signs

6.2.3. Routes and timings

In addition to a well-designed site plan, Security staff will use patrol plans that describe the routes and zones that must be patrolled, and

the timings or schedules that are to be followed. For example:

Day	Zone	Route	Time	Method
1	Perimeter	A	06:30	Vehicle
			10:30	Walking
		B	16:30	Walking
			20:30	Vehicle
		C	00:30	Vehicle
	Outer public	A	08:30	Walking
		B	11:30	Vehicle
		C	13:30	Walking
	Inner public	A	09:30	Walking
		B	12:30	Walking
	Secure	A	07:30	Walking
		B	17:30	Walking

Table 14 - Example patrol plan

The following will have been considered when preparing a patrol plan for a specific site or location:

Site layout and size

- How can 100% site inspection be achieved
- What are the most efficient routes to travel through the site

Security zones

- How is the site divided into access zones
- What controls are in place to separate the zones
- Who is likely to be present in each zone, and what threats or risks have been identified

Critical security areas

- Which areas are most critical to the organisation
- Do certain areas require rapid response capabilities in the event of an incident

Supporting technologies and systems

- What areas are covered by CCTV or sensors
- Where are access panels or alarms installed

Personnel available

- Numbers of staff available to perform patrols
- Organisational policies regarding lone workers

Shift rotations

- Timings of shift start and end
- Reduction in personnel for night shifts

Organisational timings

- When a business or organisation is open to the public
- When deliveries, maintenance or other scheduled activities normally occur

All of this information will be evaluated in order to plan a cohesive patrol schedule.

6.3. Patrol preparation

Security patrols can be divided into 3 phases:

- Preparation
- Conduct
- Completion

The preparation phase is vital to ensure the safety and success of the security patrol.

6.3.1. Confirmation of patrol requirements

The first step in the preparation phase is to confirm the requirements for the patrol including:

- **Aims and objectives of the patrol e.g.**
  - Information gathering
  - Routine inspections
  - Show of force
- **Zones and routes to be covered**
- **Key security areas to be inspected e.g.**
  - Power generation equipment
  - Life support systems
  - Hazardous waste processing
  - Fuel storage
  - Data centres etc.
- **Communications procedures including:**
  - Primary and alternate radio frequency
  - Secondary communications
  - Reporting requirements
- **Other Equipment to be carried e.g.**
  - Keys and access passes
  - Defensive tools (if required)
  - Patrol inspection checklist
  - Patrol map
  - Patrol touring device
  - Torch
  - Notebook and pen
  - Personal first aid
  - Appropriate PPE

These patrol requirements are normally outlined within a work instruction document prepared by the Security Manager.

6.3.2. Equipment preparation and testing

Key information

Having confirmed the requirements of the patrolling activity, thorough equipment preparation and testing must be carried out to reduce the risk of failure while on patrol. A pre-patrol checklist can be developed to guide and assist Security staff in carry out the appropriate checks and tests

A good practice for pre-patrol checks:

Item	Check
Keys & Passes	Correct for zones and patrol route
	Signed for in key register
Radio	No damage to body
	Antennae fitted in good condition
	Buttons and switches normal operation
	Battery charged, and spare available
	Correct frequencies programmed
	Accessories fitted in good condition e.g. ▪ Belt clip ▪ External microphone ▪ Earpiece
	Signed for in post equipment register
Duty belt	Pouches in good condition
	Baton loop securely fitted
	Buckle in good condition
	Signed for in duty post equipment register
Plastic handcuff	No deterioration of the plastic material
	Locking teeth function
	Signed for in restricted item register
Pepper spray	Shots remaining
	Arm/Disarm lever working
	Signed for in restricted item register
Baton	No cracks or rough edges
	Signed for in restricted item register
Patrol touring device	Battery charged
	On/Off operation
	Registers home point
	Signed for in post equipment register
Personal first aid	Kit contents in date and complete
	Signed for in post equipment register
Torch	Batteries in good condition
	Bulb/LED operational
	Case or pouch in good condition
	Signed for in post equipment register

This systematic approach to checking and testing equipment will reduce as much as possible the chance of equipment failure, and increase the odds for a successful security patrol.

Safety!

Security staff must be aware of organisational OHS policies. Depending on the place of duty PPE inspection may include:

Dangerous noise levels

- Hard hearing protection rated to decibel levels required
- Soft hearing protection requirement
- Time of exposure limits

Traffic safety

- Hi-Visibility vests, with reflective panels
- Illuminated traffic rod (red/green)
- Traffic cones

Industrial machinery and Plant equipment

- Safety boots
- Hard hat
- Eye protection rated for projectile risks

Flammable environments

- Flame resistant clothing

Ionising radiation exposure

- Dosimeter badges

Any Security staff who patrol through zones or areas with health and safety risks present must adopt the appropriate PPE levels whilst exposed to those risks.

6.4. Conducting security patrols

Procedures for conducting security patrols may be different depending on the site or organisation. Specific instructions for the conduct of patrols will be given for each location or organisation, and Security staff must be familiar with the relevant procedures.

6.4.1. Communications with control room

Communications while on patrol are essential in order to send or receive information, request assistance, or report risks and threats. Before leaving to conduct a security patrol, the following steps should be taken:

- Perform a radio communications check with the control room ensuring:
  - Signal strength is good
  - Your callsign is identified
- Advise the control room of the planned route
- Advise the control room that patrol is now commencing at the current time

6.4.2. Patrol events

While on patrol Security staff will complete a series of checks to ensure the safety and security of the site. The events that take place will differ depending on the specific site, however the most common events include:

Topic focus

- **Safety inspections**
  - Fire exits clear of obstructions
  - Fire alarm panels operating correctly
  - Fire extinguishers in correct location and in good condition
  - General health and safety hazards
- **Security inspections**
  - Doors and windows secured
  - Areas not covered by CCTV checked
  - Parking areas checked for violations or suspicious activity
  - Personnel within access zones are authorised (I.D worn)
  - Access zone controls are working correctly
  - Site perimeter is secure
  - Suspicious items or occurrences
- **Human interaction**
  - Gauge behaviour of colleagues and staff
  - Gauge behaviour of public
  - Observe relationships and interactions
  - Observe body language and non-verbal communications

Make sure to follow the patrol route in order to ensure that no areas are left uninspected

The security patrol is an excellent opportunity to gather information on the state of safety and security at a site, and the use of detailed note taking, photography and completion of inspection checklists is essential in providing the control room and security managers with useful information for decision making.

6.4.2.1. Progress reporting

Most sites and organisations will require security patrols to report on progress. The details required may be different depending on the site. The reasons for progress reporting include:

- **Security staff safety**
  - Control room know the location of patrolling staff
  - Support is able to be sent accurately
- **Situational awareness**
  - Control room aware of security status within the site
  - Able to take pro-active steps to prevent possible security risks
- **Time management**
  - Completion of patrols may be time sensitive
  - Patrolling staff may have other duties to move on to
- **Record keeping**
  - Progress reports will be logged
  - Evidence of duty being performed

6.4.2.2. Responding to unplanned events

During the conduct of security patrols, there may be unplanned events that require the response of patrolling staff. This could include:

- Discovery of security breach
- Discovery of immediate health and safety concern
- Extra support required at another location

In the event that patrolling staff are required to respond, the following should be completed:

- The control room must be notified
- Progress noted regarding the current patrol

This will enable the patrolling task to be completed accurately when the unplanned incident has been resolved.

6.4.3. Patrol completion procedures

Upon completion of a security patrol, staff must follow a post-patrol procedure. This will ensure that the benefits of the patrol activity are gained. Typical patrol completion procedures include:

Return of Equipment

- Inspect all patrol equipment for damage and wear
- Sign in any patrol specific equipment
- Place any powered items on charge
- Sign in and secure restricted items

Patrol notes and reports

- Review patrol notes for accuracy
- Ensure any patrol checklists are complete
- Prepare a patrol report if required
- Submit patrol documentation to the control room

Patrol duty handover

- Verbal briefing of oncoming patrol staff
    - Significant observations
    - Incidents if any
    - Routes taken during previous patrol
    - Specific tasks uncompleted

The patrol completion requirements may be different depending on the type and scale of the site or organisation, but following this method as a basic guide will ensure smooth security patrolling operations.

6.5. Key and critical areas

Key and critical areas are those which are essential to the continuous operations of an organisation, or that interference with would cause harm to people, property or information.

6.5.1. Critical area knowledge

Security staff must possess detailed knowledge of critical areas within the site they are tasked to patrol, in order to properly understand the primary aims of the security patrol. Critical areas specific to each site will be different, but as a general guide the following could be included in a critical area list:

- Heating, Venting and Cooling machinery
- Power supply access
- Water and utilities access
- Hazardous materials storage
- Medical waste disposal systems
- Oil, Gas or Petroleum pipelines
- High value goods storage
- Data storage centres
- Site entry and exit points
- VIP offices or accommodation
- Perimeter zones
- Essential operations zones e.g.
    - Airport runways & aprons
    - Manufacturing rooms
    - Import/export yards and terminals

Any area specified by the business or organisation as essential to their success may be a critical area.

6.5.2. Determining security status of critical areas

In order to conduct security inspections of critical areas within a site, patrolling staff must understand what is the 'normal' state for that area. This knowledge will usually be gained during a site induction conducted by the site security supervisor or manager.

Topic focus

Some basic considerations that may apply include:

- Obvious damage to equipment or infrastructure
- Liquid leaks or escaping gases
- Signs of forced entry, or unsecured access points
- Loss of power or other utilities
- Suspected unauthorised persons in the area
- Obvious missing items e.g. Generators, Computer servers, electrical cabling etc.
- Open access gates

It should be a priority of new Security staff to learn and understand the critical security areas within a site and what the normal state of operations looks like.

While on security patrol, Security staff will report to the control room on the current status of identified critical areas to provide real-time updates on the status of these areas within the site

6.6. Building searches

Security patrolling staff may be required to search buildings and structures within the site in response to reported information, or as a routine task.

6.6.1. Building search requirements

Establishing the purpose for searching a building will provide the patrolling security staff with essential information that will help them to make decisions about personal safety, and contribute to a successful building search.

6.6.2. Planning to search a building

When planning to conduct a building search the following considerations can be made:

- Entry and exit locations
  - Enabling escape of suspects
  - Calling in further support
  - Enabling retreat of security staff
- Stairwell locations
  - Enabling transit within a multi-floor building
  - Provide escape routes for suspects
  - Provide choke points for inner-cordon during search
- Number of floors
  - May dictate the size of search team
  - Enabling 100% search coverage of the building
- Building purpose e.g.
  - Office space
  - Storage
  - Plant and Machinery housing
  - Warehousing

6.6.3. Building search safety considerations

Before entering a building to conduct a security search, safety must be given priority. The following areas should be considered, and a quick risk assessment performed:

- **Security circumstance of search**
  - Suspicious person inside
  - Suspicious item inside
  - Suspicious activity near the building
  - Aggressive person inside
- **Health and safety**
  - Lighting conditions inside
  - Low doorways, piping or conduits
  - Trip hazards
  - Hazardous substances
  - Presence of fire or gas
  - Available exits in case of emergency abandonment of search
- **Communications plan**
  - Radio coverage inside building
  - Use of runners to relay search progress
  - Alternate communications in case of failure

Security staff should assess the presence of these risks to personal safety and the safety of the team, and take appropriate precautions and use the correct PPE before conducting the building search.

6.6.4. Searching with other security staff

Depending on the size of the building, threat level and available security staff, a building search may involve a larger search team. The main principles of searching as a team are as follows:

- **Communication**
  - Radio, visual, or verbal
  - Brief and relevant to search task
- **Coordinated movements**
  - 1 person in charge
  - Methodical progress through building
  - Clear by sections before moving on
  - Single floor at a time if multi-floor building

- **Maintenance of a cordon**
    - Use of Security staff to cordon access to the building
    - Prevent others from entering
    - Prevent suspects from escaping

The use of training drills and practice will enhance a search teams' efficiency and skill in quickly and accurately completing a search of a building. Security staff should be familiar with the layout of all buildings within their site.

6.6.5. Use of canines for building searches

Trained canines can be used as a tool to assist in the search of buildings. Depending on the scenario, and what is being searched for, a canine may provide excellent support in the form of:

- Confirming the presence of explosives
- Confirming the presence of narcotics
- Personnel tracking / missing person trace
- Cadaver detection (Deceased persons)

Key information

For the effective use of canines in search, it is important to reduce contamination of the area with further human scents.

Some further basic rules for canine search operations include:

- Do not approach the dog for petting
- Do not feed the dog
- Do not distract the dog handler
- The dog can only work for short intervals effectively
- Environmental conditions will impact the duration and effectiveness of canine search e.g. heat exhaustion

Safety!

If there is any doubt about the personal safety of a high risk building search, Security staff should defer to the appropriate public security agency e.g. Police, Civil Defence, Military

6.7. Patrol documentation

Security patrolling activity is required to be documented, and as described previously, it will usually be in the form of patrol notes kept in the security notebook, completed patrol checklists, and if any incidents were dealt with, an incident report will also be completed.

6.7.1. Reporting requirements

Site duty instructions will describe the types of events, occurrences or incidents that require a formal incident report. Security staff should be prepared to keep notes on any occurrence that they believe may have an impact on the safety or security at the site.

The standard procedure for reporting is:

- Urgent incident
    - Report in real-time over radio to control room
    - Take mental notes while dealing with incident
    - Write incident details in notebook immediately after incident is resolved
    - Prepare formal incident report
    - Submit to control room
- Non urgent incident
    - Report to control room
    - Write notes in notebook
    - Include details in patrol report
- Other observations
    - Write notes in notebook
    - Include observation details in patrol report

6.7.2. Standard patrol documentation

Security staff must be familiar with the standard patrol report format that is in use at the site.

Topic focus

A security patrol report is a standard document that the Security staff will complete. The contents of a patrol report include:

- Staff name
- Staff ID
- Date
- Start time
- Finish time
- Zones/Areas inspected

- Route taken
- Security checks performed
- Security status of critical areas
- Safety inspections performed
- Observations or comments
- Signature

When completing a patrol report, accuracy is essential. Include only facts, and not assumptions. The patrol report may act as a legal document if any investigations are opened, and the contents of the report must be true.

An example of this document can be found on the next page.

Key information

Any security documents be secured in accordance with organisational policy, and information security standards. Best practice for this includes:

- Lockable filing cabinets kept in an access controlled room (control room)
- A document register kept to record files stored and removed from the cabinet
- Proper destruction of documents no longer required e.g.
    - Shredding, burning, pulping or granulation
- A record of destroyed documents kept

Example patrol report

Name				**ID**				**Signature**	
Date		**Start time**		**Finish time**		**Route**	A ☐ B ☐ C ☐	**Zones**	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

	Location	**Check**	**Security Status**		**Comments**
			✓	✗	
Zone 1	1	Fire exits			
	2	Fire extinguishers			
	3	Zones not covered by CCTV			
	4	Reception area			
	5	Fire alarm panels			
	6	VIP Carpark			
Zone 2	7	Exterior pathways			
	8	Windows and doors			
	9	Data room			
	10	HVAC room			
	11	Rear gate			
Other observations					

Module 6 Revision

Revision questions	
1. Where would the site security plans, patrol instructions and patrol maps be found? a. In the main reception b. In the security control room c. On the company website d. In the finance office	**2.** What are the 4 P's of patrolling (Aims)
3. List 3 methods of security patrolling	**4.** List 3 crime prevention strategies
5. List the steps of the patrol preparation phase	**6.** List 5 security inspection events while on patrol
7. List the steps of patrol completion phase	**8.** Outline the information security requirements for patrol documentation

9. List 5 examples of critical areas for inspection on patrol	**10.** What are the 3 categories of safety to consider before searching a building?
11. List the 3 principles of teamwork when searching a building	**12.** Summarise the precautions that need to be taken regarding human scent when using canines for search

Module 7
Observation &note taking

Module 7

Observation & note taking

Qualification Link

Units

- Nil

Learning outcomes

1. Using the official security notebook
2. Recognising why things are seen
3. Identifying methods for keeping information in the memory
4. Using standard formats to keep incident notes
5. Using standard formats to record people and vehicle information
6. Recording witness statements and handling evidence
7. Recognising aids to recording information

Key definitions

Evidence – any sample, item or recording that will support a point of view

A fact - is any detail that can be proven to be true

An assumption - is an interpretation of a situation without definite proof

7.1. The official security notebook

Security staff are issued with an official notebook in which daily observations, incidents details, shift details etc. are to be recorded. The official security notebook must go everywhere with Security staff, and this is a requirement by the ministerial decision 557 of 2008.

7.1.1. Issue and return of the notebook

Key information

Each notebook is serial numbered, and is issued to Security staff as a controlled item. When the notebook is filled, it will be returned through the company and a new notebook issued.

7.1.2. Legal status and care

The official notebook must be cared for as it holds status as a legal document, and may be requested as evidence in court cases following a serious incident. Security staff will ensure that no pages are torn out, and that the notebook is not damaged in any way.

7.1.3. Completing entries in the notebook

Topic focus

When completing entries in the official notebook the following basic principles should be followed:

- **Be clear** – write down the exact circumstances of any incident or observation
- **Be concise** – don't use more words than necessary, get to the point
- **Be consistent** – complete each entry in the same format
- **Be complete** – don't leave out any of the required information
- **Be factual** – include only facts, not assumptions about what has happened

Security duty should be recorded in the notebook using the following details:

- Date
- Day of the week
- Duty post
- Equipment received
- Shift supervisor name
- Time started
- Time finished
- Weather conditions (if outdoor duty)

When recording duty observations in the notebook:

- Do not leave any blank pages or spaces on a page
- Use a black pen
- Use the margin to record the time of each entry

Anything interesting or unusual, possibly of future importance, actions taken or incident related should be recorded for reference

Figure 58 - Note taking

7.1.4. Standard methods for note taking

When taking notes on observations or incidents, a good practice is to describe events using the following format:

- **At date**
- **At time**
- **What happened**
  - What was observed
  - Who was involved (list all persons)
  - Where did it happen
  - Why did it happen
- **What was done about it**
  - Were actions required
  - Response taken
  - Support requested
- **What was the outcome**
  - Was resolution achieved
  - Were there consequences
  - Have normal operations resumed

If an incident is ongoing, Security staff should deal with immediate issues and make a mental note of the time each event is occurring. The events should then be entered into the notebook using the format as described, in a timeline.

An example of a notebook entry:

1-1-19 0900	2 vehicles were involved in an accident. The driver of a red Toyota Camry, registration 12345 was Mr. Mohamed Al Ali. The driver of the white Nissan patrol, registration 4321 was Mr. Ali Al Kaabi. The accident happened at the main gate. It happened because the white Nissan patrol turned in front of the red Toyota Camry without signalling.
0901	Both vehicles were directed to park at the side.
0902	The police were called
0915	The police arrived
0925	Both drivers completed the paperwork with the police
0930	The police left the site
0931	Both vehicles drove away with minor damage
0932	Normal operations resume at the main gate

7.2. Human senses

While on duty, Security staff can make use of the human senses to assist in detection of possible risks or dangers.

Figure 59 - The 5 human senses

7.2.1. The 5 human senses

The human senses are divided into 5 categories:

- **Sight -** Enables the Security staff to detect through visual perception
- **Hearing** – the ability to detect crime or threats through audible sounds
- **Smell** – Able to detect unusual occurrences or clues to a change in the environment through scents
- **Touch** – Ability to detect clues to a crime or hazards and risks by touching surfaces, substances, packages and people
- **Taste –** This sense will have limited use in the detection of security issues

The use of the human senses is an instinctive ability, however Security staff can remain mindful of the abilities they have and make use of any advantage that multiple sense can offer in the detection of security risks, hazards or criminal activities.

7.2.2. Why things are seen

Key information

Humans are able to detect visually in response to 6 characteristics which are:

- **Shape** – the lifetime of experience has built a mental library allowing recognition by the shape of an object
- **Shadow** – the casting of shadow will draw the attention of an observer
- **Surface** – the material surface of an object may shine or contrast with the surrounding environment
- **Spacing** – objects that are uniformly spaced will draw the attention of an observer, as naturally occurring features are never spaced out evenly
- **Silhouette** – A familiar or recognisable silhouette will stand out
- **Movement** – the strongest of all, movement will immediately draw the eye of an observer allowing an object to be detected

Knowledge of why objects are seen, and a conscious application of these principles will assist Security staff to make best use of their visual perception in the detection of any security risks, locating evidence, watching for danger or identifying hazards.

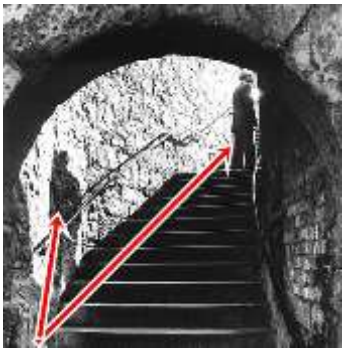


Figure 60 - Example of detection by shadow

7.3. Remembering details

The ability to remember details is an essential skill for Security staff. Practice and training can assist in developing this ability, and the use of techniques to help recall details can be used to good effect.

7.3.1. Techniques for retaining information

An effective method of retaining information and details is to construct a storyline that involves each piece of information, so that when required the details can be reconstructed following that storyline.

This method can be used to recall lists of items observed by placing each item into a story that is made up, making it easier to retrieve each item from memory as the story is retold.

For example:

Items required to be remembered
▪ Rope
▪ Plastic bag
▪ Knife
▪ Wire cutters
▪ Mobile phone
▪ Petrol can
▪ Water bottle

Storyline:

I was riding my motorcycle when it ran out of petrol so I called my friend on a **mobile phone** and asked him to bring me a **petrol can**. He put it in a **plastic bag** and used a **rope** to tie it to his motorcycle. When he arrived I gave him a drink from my **water bottle** and tried to cut the rope with **wire cutters**, but he said it would be better to use a **knife**.

7.4. Noting observations

When making note of observations in the security notebook, it is essential to record details in methodical and unbiased way.

7.4.1. Facts vs assumptions

Notes should be stated as facts, and making assumptions about any situation should be

avoided. Facts can be assessed objectively by any person who will read the notes at a later time, but assumptions made by Security staff will lead to a bias or preconceived assessment being made by any person who reads the notes.

- **A fact** is any detail that can be proven to be true
- **An assumption** is an interpretation of a situation without definite proof

Security staff must maintain the ability to observe and record facts in order to present the most accurate account of events. An example of this could be:

Fact	Assumption
There are currently no clouds in the sky	The weather will be good today
The man was shouting and held his fists by his side	The man was planning to assault the Security guard
The gate was found unlocked	A criminal had broken into the premises

7.5. Describing people and vehicles

Security staff will frequently be required to note the details of people and vehicles during daily duty to support the passage of information, investigations or incident reporting. Several methods have been developed to assist in capturing useful descriptive information about people and vehicles.

7.5.1. Recording details about people

The method developed for recording details about a person is known as the "A to H" method. Security staff can quickly call upon this format to collect the most accurate description of a person

Topic focus

When recording details about a person, identify:

A – Age (within 2 years + or -)

B – Build (fat, thin, muscular etc.)

C – Clothing

D – Defining features (Tattoos, scars, jewellery etc.)

E – Elevation (height of the person)

F – Face (shape i.e. long, square, round)

G – Gait (how they walk, limp etc.)

H – Hair (colour, length)

Following this format will allow Security staff to quickly and accurately record and pass along descriptions of people

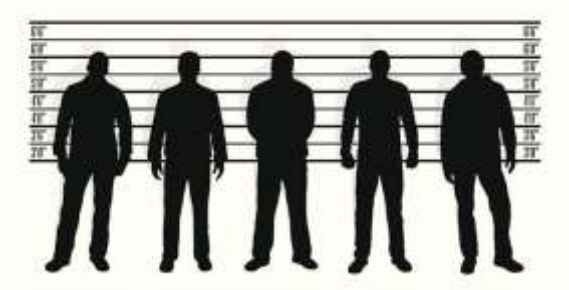


Figure 61 - Identifying personal features

7.5.2. Recording details about vehicles

The method used to record details about vehicles is known as "SCRIM" and is a quick format that can be used reliably to record and pass on information.

Topic focus

When recording details about vehicles, identify:

S – Shape (Sedan, SUV, Truck etc.)

C – Colour

R – Registration (Plate number and Emirate)

I – Identify features (Scratches, dents, smoking exhaust, upgraded parts etc.)

M – Make and model

Following this format will allow Security staff to quickly and accurately record and pass along descriptions of vehicles

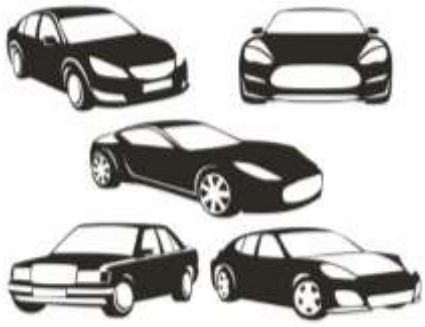


Figure 62 - Identifying vehicle features

7.6. Witness statements and evidence handling

Security staff may be required to take statements from witnesses after an incident has occurred, and there are several considerations that should be made during this process

7.6.1. Taking witness statements

When taking statements from a witness Security staff should:

- Record the date and time of the statement
- Give the context of the statement in relation to any incident or occurrence
- Write the statement in the first person i.e. from the perspective of the witness
- Read the recorded statement back to the witness and offer the opportunity to make amendments
- Ask the witness to date and sign the statement

Depending on the situation and type of occurrence, Security staff may also need to be aware of:

- Witnesses in a state of shock – care for and treat appropriately as a priority, wait for the witness to return to a normal state of mind
- Collaboration between witnesses – Separate all people directly involved in an incident and take their statements in isolation to avoid the opportunity to create an untrue story between witnesses

When interviewing the witness to take their statement, Security staff should ask:

- Where were you located
- What did you see (Facts only!)
- A diagram could be drawn by the witness to provide further clarity on locations of all events

Witness statements may be used by the Police to further assist during investigations, and the accuracy of these statements is very important. Security staff should be well practiced in taking witness statements.

7.6.2. Handling evidence

In the event of any accident, incident or crime, the police should be the first agency to handle the processing of any evidence. There is the possibility that some situations may require Security staff to handle evidence, and the correct process and procedure should be followed.

Key information

Incident scene management

Security staff may be required to control access to and handle evidence of a crime or incident. In order to effectively secure evidence, the following principles of incident scene preservation should be followed:

- **Prevent scene contamination**
  - Keep personnel accessing the incident site to a minimum
  - Keep a log of any personnel entering the incident site
  - Prevent additional items or objects from cluttering the scene
- **Prevent evidence destruction**
  - Preserve any items of evidence from being destroyed e.g. shelter from wind or rain
  - Prevent deliberate sabotaging of evidence through controlling the site
- **Prevent evidence movement**
  - Prevent items of evidence from being moved within the incident site
- **Prevent evidence removal**
  - Ensure that evidence remains at the incident site, and is only removed by authorised personnel e.g. police, crime scene investigator etc.

Figure 63 - Incident scene preservation

If Security staff are required to physically handle and document evidence for later processing or handing over to the Police, the following procedures should be followed:

Topic focus

Handling of evidence

The following six steps should be followed when physically handling any type of evidence:

- **Collection**
  - Wear gloves to prevent contamination of the evidence
  - If more than one item of evidence is collected, change gloves in order to maintain a sterile connection to the evidence
  - If evidence is a substance, collect a sample on a sterile swab and place into a zip lock bag
- **Securing**
  - Prevent any further access to the item of evidence
- **Preservation**
  - Keep the evidence in an appropriate environment to preserve the usefulness at a later time
- **Identification**
  - Label the evidence bag with Company name, Staff name, date, time, location and evidence number
- **Continuity of custody**
  - Ensure a record is kept of the transfer of evidence from one person to another
- **Logging**
  - Document all items of evidence in a evidence register

Security staff should always let the Police handle evidence as the first priority. Only if circumstances require immediate intervention in order to preserve the evidence should Security staff handle any evidence

Figure 64 - Collected evidence example

7.7. Aids to recording information

There are many systems available to assist Security staff in the accurate recording of information at their site.

7.7.1. Recording technologies

Taking advantage of modern technologies can prove useful in the collection and storage of high quality information. Examples of this include:

- **Body cameras**
  These small rechargeable cameras can be worn on the uniform of Security staff to capture evidence while the staff are on duty
- **Hand held cameras**
  A hand held camera can be carried and used to take photos to support incident reports, maintenance reports or other documentation and filing systems used within an organisation
- **Mobile phones**
  Carried by all Security staff, mobile phones can be used to record video, take photos and record audio (witness statements etc.)

- **CCTV footage**
  Relevant sections of recorded video can be extracted and attached to incident report files. Still images can be captured and used to enhance reports
- **Audio recorders**
  Dictaphones can be used to capture interview audio for later accuracy in report writing
- **Aerial surveillance footage (drones)**
  An accurate overview of a situation can be captured using aerial footage, with the video recorded for later viewing
- **Guard touring applications (mobile phone)**
  Security staff can capture video or still images, audio recordings and notes directly into an information sharing app for rapid distribution within the security team, and directly fed into report templates

Body camera

Guard touring app

Aerial drone

Hand held camera

Audio recorder

CCTV

Module 7 Revision

Revision questions

1. When starting duty, what information should be recorded in the official notebook

2. What 6 characteristics allow for visual detection

3. When recording information about a person, what does A to H mean

4. When recording information about a vehicle, what does SCRIM mean

5. List the 6 steps of evidence handling

Module 8
Traffic management

Module 8
Traffic management

Qualification Link

Units

- SEC04003NU18-Implement site traffic management procedures

Learning outcomes

1. Interpret traffic management plans
2. Enforce traffic management plans
3. Identify types of traffic
4. Identify parking zone technologies

Key definitions

Traffic – the passage of people or vehicles along designated routes

SCRIM – Size, Colour, Registration, Identifying marks, Make and model of a vehicle

8.1. Site traffic plans

Security staff will be responsible for the safe and secure movement of all traffic types that are within, and accessing their place of duty. It is important that Security staff are aware of the site traffic plan, and what is required to enforce it. A traffic management plan will be kept in the Control room for staff to access and use as reference.

8.1.1. Traffic plan contents

A site specific traffic plan will be produced by the HSE and/or Security manager for that site, and normally will include the following information:

- Categorisation of traffic types
- Traffic access permissions
- Route restrictions for traffic type
- Hours of operation for entry points
- Traffic mixing risk assessment (people, vehicles etc.)
- Parking locations and restrictions
- Enforcement and escalation procedure

Some of the information contained in the plan will be taken from access control policies for the site and applied to the traffic management plan

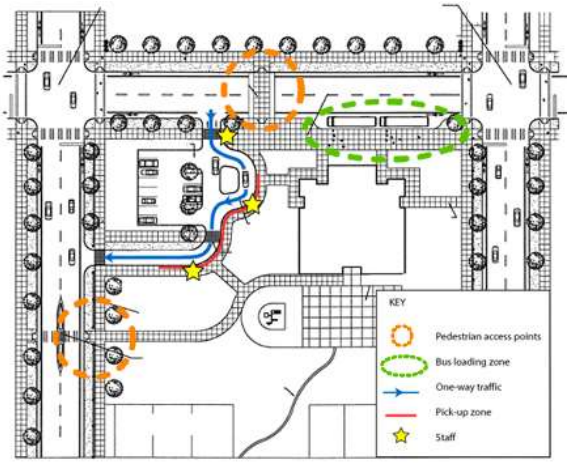


Figure 65 - Example traffic plan map

8.2. Traffic categories

Security staff must be able to identify the different types of traffic expected to be using the site. The exact categorisation will depend on the specific site, but a logical method will be used to define what type of traffic can move where.

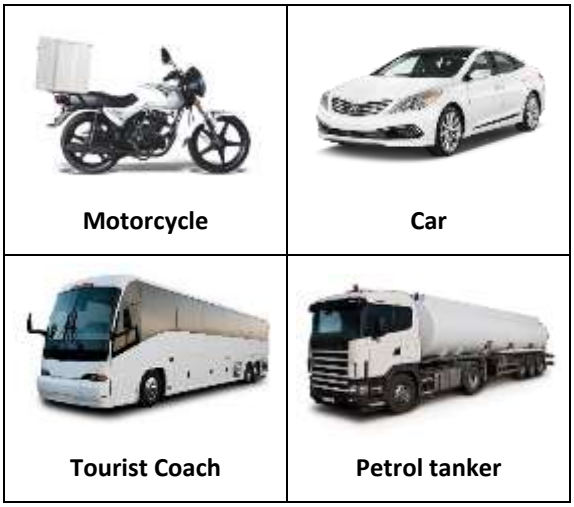


Figure 66 - Example traffic types

8.2.1. Categorising traffic

Key information

Simply put, traffic can be placed into 2 categories:

- Vehicle
- Pedestrian (foot)

These 2 major categories can then be divided further according to the following specifications:

- **Vehicle**
  - Light vehicle e.g.
    - Cycles
      - Motorcycles
      - Bicycles
      - Tricycles
    - Cars
      - Sedan
      - Wagon
      - Van
      - SUV
  - Medium vehicle e.g.
    - 20 seat coach
    - Flatbed truck
    - Ambulance
    - Forklift
  - Heavy vehicle e.g.
    - Tourist coach
    - Fuel tanker
    - Cement truck
    - Fire truck
  - Special purpose
    - Hazardous material transport
    - Wide load transport
    - Crane
- **Pedestrian**
  - Able bodied
  - Elderly
  - People of determination

This list is not complete, but provides a good understanding of how to think about the different types of traffic that may be using a site.

8.2.2. Separation of traffic types

In order to maintain safety and security within a site, it may be necessary to separate traffic types from coming into contact with one another. Examples of this may include:

- Hardened barriers between pedestrian walkway and vehicle routes
- Markings painted on pavement requesting bicycles and pedestrians keep to either side
- Bollards between parking areas and public waiting areas
- Separate access lanes for heavy vehicles and light vehicles

The decision to separate traffic types from one another will normally be taken as a result of a risk assessment being performed.

Security staff should be aware of control measures used within the site to separate different traffic types, and ensure that they are used appropriately to maintain safety and security

8.2.3. Routes and restricted areas

A good site traffic management plan will include a site map with approved traffic routes and restricted areas marked for simple identification, for example:

- Ambulance loading zones at hospitals
- Passenger pick and drop zones at airports

Figure 67 - Ambulance arrival area

Figure 68 - Passenger drop at airport

Security staff must have a strong knowledge of what type of traffic is permitted to travel along routes within the site, and understand restrictions in order to properly enforce the traffic management policy.

8.3. Parking management

Parking management is a common part of traffic management at a site, as most traffic will end up parking somewhere within a site. Understanding what type of traffic can park where, will enhance the Security staff ability to maintain security.

8.3.1. Purpose designed parking zones

Parking zones may range from informal locations that have evolved from the habits of users, up to purpose designed spaces engineered to handle vehicles a certain specification.

Parking zones may be laid out as:

- Multi storey
- Open
- Kerbside

The characteristics of a well-designed parking zone include:

- Blast safety distance from priority assets or buildings
- Enough space to manoeuvre a recovery vehicle
- Parking bays clearly marked
- 100% CCTV monitoring
- Well lit
- Location clearly sign-posted
- Limits and restrictions clearly sign-posted

Figure 69 - Example car park design

A well-designed parking zone will encourage users to follow parking procedures, and make the job of Security staff simpler

8.3.2. Parking zone technologies

There are many available systems and technologies to assist in the management of a vehicle parking space.

Frequently used in public car parking spaces

- Access control
  - Automated barrier arm
  - Pop up bollards
- Parking duration monitoring
  - Number plate recording
  - Access token
  - Barcoded ticket
  - Parking bay sensors
- Occupancy management
  - Automated zone closure
  - Empty bay indicators
  - Empty bay counters

Access control and ticketing

Occupancy management

Figure 70 - Car park technologies

Many of these systems can be integrated and monitored centrally from the site security control room. Security staff will routinely inspect parking zones as a part of the mobile patrolling plan in order to:

- Ensure the vehicle type is permitted to park
- Verify authorisation of parked vehicles
- Deter antisocial or criminal behaviour
- Enforce time limits
- Identify suspicious vehicles or security risks
- Identify health and safety concerns
- Maintain situational awareness within the site

8.4. Enforcing traffic management policies

Security staff are empowered by organisational management, and in some cases civil law to enforce traffic policy at a site. Confidence and authority to direct traffic, report violations, and take action against non-compliance is essential.

8.4.1. Directing traffic

There may be occasions when Security staff are required to give manual directions to traffic at a site. Examples of this may include:

- Directing traffic through an entry or exit point
- Directing traffic flow around an obstacle
- Marshalling vehicles toward a parking zone

Key information

When directing traffic:

- Give directions from the front of the vehicle – NOT behind
- Use large exaggerated movements
- Maintain eye contact with drivers
- Restrict the flow to a manageable rate for colleagues to perform other duties e.g.
    - Checking ID
    - Searching vehicles
    - Giving site induction briefings
    - Marshalling into parking bays
    - Etc.

It is important that Security staff are able to give clear and decisive direction, and a set of principles and hand signals have been developed for this purpose

Safety!

When on traffic direction duties always:

- Wear a Hi-Visibility vest
- Carry a whistle for gaining attention
- If working at night, carry a torch and traffic wands (red/green)
- Maintain spatial awareness
- Identify an escape path if a vehicle is out of control

In order to direct traffic movement, 6 basic manoeuvres have been identified, and the corresponding hand signals created.

Proceed slowly forward:

- Both arms raised with the palms of hands facing direction of required vehicle movement
- Bend both arms repeatedly toward the head and chest

Figure 71 - Direct traffic forward

Move backward:

- The same movement as moving forward, but with the palms facing forward

Figure 72 - Direct traffic backward

Make a turn:

- Point one arm to the direction of the turn
- Bend the other arm repeatedly toward the head to indicate continued turning

Figure 73 - Direct traffic right

Figure 74 - Direct traffic left

Clear to leave the area:

- Point at the driver to gain attention
- Turn and extend both arms in the direction to exit

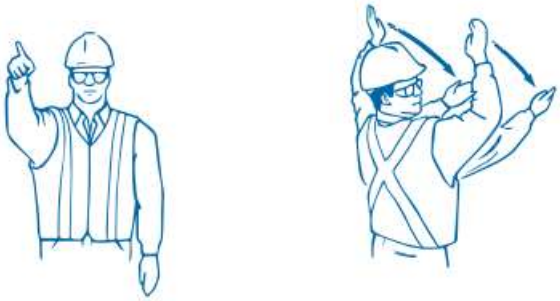


Figure 75 - Direct vehicles to leave an area

Stop:

- Cross both arms above the head

Figure 76 - Direct a vehicle to stop

Emergency stop:

- Start with hands clasped above the head
- Extend down and out to the side repeatedly

Figure 77 - Signal an emergency stop

Security staff must be well practiced in giving these signals clearly, and without hesitation. Confusing or unconvincing directions may cause injury or even death.

Key information

If giving directions with a set of traffic wands, ensure:

- Only activate green light to give movement directions
- Use red light to communicate no movement authorised.

Figure 78 - Example of green/red traffic wand

8.4.2. Delivering site inductions

Certain sites may require that visitors receive an induction briefing notifying them of how they must act while on the site. Typical sites that may require this include:

- Construction sites
- Industrial complexes
- Airside areas within airports
- Sea ports
- Energy production and refinery sites

The complexity of a site induction will normally depend on the type of visitor or site user, and the risk factors present on the site. Induction briefings may be as simple as giving instructions to a driver through the vehicle window, or could be a fully planned training session for permanent staff using vehicles within the site.

Topic focus

To deliver a brief site induction at the point of access, Security staff should explain at a minimum:

- ID to be displayed (vehicle pass and visitor badge)
- Routes permitted to use within the site
- Parking zones permitted within the site
- Restricted areas not to be approached
- Actions to take in the event of an accident or breakdown
    - Security contact number
    - First aid locations
- Site exit procedure including:
    - Return of passes and badges
    - Vehicle search requirements

For a high risk site, the organisational management may require signed documentation acknowledging the receipt of an induction briefing by Security staff.

In order to effectively communicate the required information, Security staff should keep on hand:

- A site map with non-restricted information marked on it
- A checklist with required information to be communicated

Critical details can be printed on the vehicle passes issued, for easy referral by the driver while on site

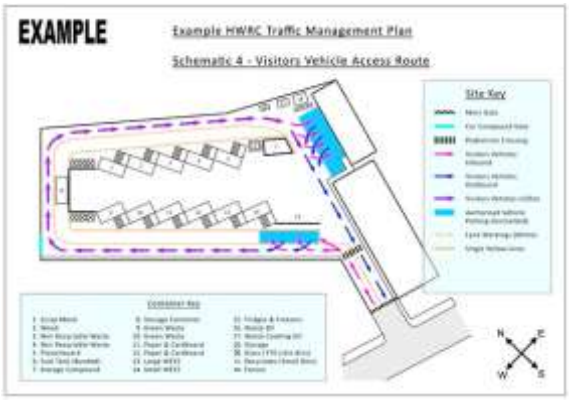


Figure 79 - Map used to direct visitors

8.4.3. Identifying traffic non-compliance

Being very familiar with the site traffic rules and management policy will allow Security staff to identify any instances of non-compliance, enabling the correct response procedures to be taken. Specific responses will depend on the organisation and site, but common actions in response to non-compliance with site traffic policy could include:

- Verbal warnings to drivers
- Drivers sent off the site
- Drivers restricted from entering the site in the future
- Clamping of vehicles
- Triggering of vehicle search policies e.g. if a vehicle is found to have been in a restricted area
- Law enforcement action against traffic violations

Figure 80 - Example of wheel clamping for non-compliance with parking regulation

8.4.4. Reporting site traffic violations

Security staff will immediately report any site traffic violations identified to the control room for situational awareness. A record should be kept in the official notebook for later transfer into a daily occurrence report. When reporting traffic violations, the SCRIM description for vehicles can be used, along with the standard incident reporting format described in the observation and note taking module.

Site traffic violation report	
At Date	16-01-2019
At Time	20:30
What happened	Mr Saif Al Ali, riding a motorcycle, Red, Plate 1234, Pizza hut delivery box on the back, Honda 125cc was stopped by Security staff Mr Mohammed Al Kaabi ID 4321 for riding on the footpath next to the main office in violation of the site traffic policy
What consequence	No consequences, however could have hurt pedestrians using the footpath
What action taken	Mr Saif Al Ali was given a verbal warning, and his details logged for future reference

Table 15 - Example site traffic violation report

All types of site traffic violation must be reported as it will help the HSE and Security management to:

- Identify trends in traffic incidents
- Produce updated risk assessments
- Maintain situational awareness within the site
- Prepare accurate reports for PSBD Operations

Module 8 Revision

Revision questions

1. List 5 pieces of information that will be contained within a site traffic management plan

2. List 3 examples of a light vehicle

3. Outline the information to given for a site induction to a driver through the window

4. List 3 types of site that may require a site traffic induction

5. Draw the signal used to direct a car to the right

6. List 3 pieces of safety equipment to be used when directing traffic

7. List 5 features of a well-designed parking space

8. Explain the main reason for separating different types of traffic when moving through a site

9. True or False. Vehicle directions are always given from behind the vehicle

   TRUE / FALSE

10. When giving direction to traffic, the palms of the hand must:

    a. Face the ground
    b. Face the direction of required movement
    c. Face upwards

Module 9
Vehicle searching

Module 9

Vehicle searching

Qualification Link

Units

- SEC03003NU18-Use security search methods and equipment

Learning outcomes

1. Interpret search policies and procedures
2. Select and use security search equipment
3. Search vehicles

Key definitions

Search bay – an area specifically designed to carry out vehicle searches

Traffic controller – the person responsible for directing vehicles forward in a queue to be searched or not

Searcher – the person or people responsible for physically inspecting the vehicle

9.1. Vehicle search laws and regulations

As with searching people, the legal authority for Security staff to search a vehicle is only by consent.

9.1.1. Authority to conduct searches

Key information

When on duty as a vehicle searcher, Security staff must inform drivers if a search of the vehicle is a requirement of access to a site or area. This can be achieved through verbal communication or signs. Points to note for security staff include:

- Driver may refuse vehicle search request
- Security staff may deny access without vehicle search
- Refusals of search request should be documented and reported

9.2. Vehicle search policies

Organisations will provide Security staff with policies that will guide the vehicle searching requirements for the site or area. Information contained within the vehicle search policy will include:

- **Selecting vehicles for search e.g.**
  - All vehicles entering the site, e.g. 20% random search
  - All vehicles exiting the site, e.g. 100% search
  - Specific vehicle types, e.g. Delivery vans must be searched on entry
  - Specific driver types, e.g. unplanned visitors' vehicles must be searched
  - Locations to be visited, e.g. vehicles that will access sensitive areas within the site are to be searched
- **Driver management during search e.g.**
  - Remaining in the vehicle
  - Separated from vehicle
  - Separated from vehicle, and kept from view of the search process
- **Level of detail e.g.**
  - Visual search of interior
  - Visual search of boot
  - Physical search of all compartments and cavities
  - Underside inspection
  - X-Ray of entire vehicle
- **Refusal of search requests e.g.**
  - Reporting requirements
  - Actions to take e.g. denial of entry or exit
- **Prohibited items e.g.**
  - What to look for
  - What to do when prohibited items are found
- **PPE and search tools required e.g.**
  - Personal safety equipment to be used
  - Technologies and equipment to be used

Security staff will need to be familiar with the requirements for the particular site at which they are working, and copies of vehicle searching policies can be found in the Security control room for reference.

9.2.1. Selecting vehicles for search

Depending on the size of the Security team, the responsibility to select which vehicles need to be searched may fall to the Traffic controller, who then directs vehicles into the search bay, or the searcher themselves who is working without the assistance of additional team members.

Key information

Regardless of who makes the selection of which vehicles to search, it must be in accordance with the site vehicle search policy, and the following should be noted:

- Always request permission to perform the search, informing the driver of their right to refuse
- Explain the consequences of refusal
- Log the details of each vehicle that has been searched

Figure 81 - Car entering search lane

9.2.2. Dealing with search refusals

If a driver refused to consent to a search of their vehicle, Security staff must understand the process to follow. Depending on the organisation and risk assessments in place, Security staff may deny access to a site, or escalate to a supervisor or manager who will then take the decision to deny access or allow the vehicle to proceed.

If a driver refuses to have their vehicle searched, the Security staff should attempt to record:

- Date, time and location
- Circumstances of refusal i.e.
    - Vehicle selected using search policy
    - Search requested due to suspicious activity etc.
- The driver's details
    - Name and ID
    - Appearance (A to H)
- Vehicle details (SCRIM)
- Stated reason for refusing search
- Actions taken upon refusal e.g.
    - Escalation to supervisor
    - Immediate denial of access

Security staff must be confident in their decision making, and enforce the established vehicle search policy

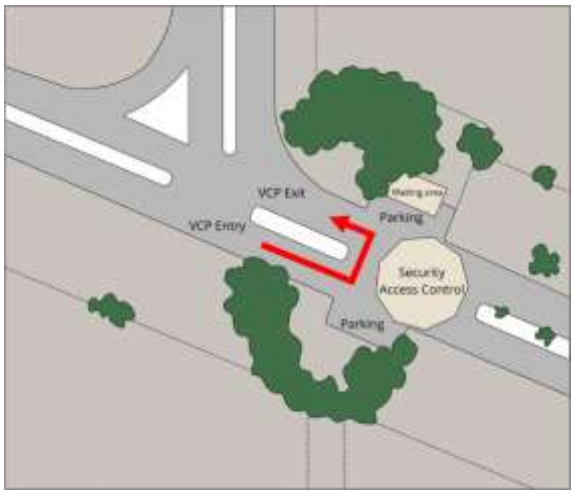


Figure 82 - Search request refusal turn around

9.3. Establishing vehicle search areas

In order to safely and effectively carry out vehicle search activities, an area should be prepared for this purpose. Security staff on duty at a vehicle search bay must understand the physical requirements of this space specific to the searching actions to be carried out.

9.3.1. Search bay design considerations

When setting up a vehicle search bay there are several major factors that will need to be considered:

9.3.1.1. Risk and threat levels

Direct violence

- Explosive devices
- Vehicle ramming

Answers to these threat levels will assist in designing search bays that can reduce the risk as low as possible, while maintaining operational capability to proceed with searches.

Example design choices to reduce explosive devices impact:

- Reinforced concrete walls surrounding individual search bays
- Electronic countermeasures to jam detonating signals
- Search bay located sufficient distance from traffic holding point
- No mobile phone use in the checkpoint
- Minimal staff inside the search area at any time (reduce exposure to risk)

Example design choices to reduce vehicle ramming threat:

- Use chicanes to reduce straight line access to the search area
- Use retractable hostile vehicle bollards or barriers to control progression into the search area

Health and safety

- Exhaust fumes
- Vehicle impact
- Environmental exposure

These hazards could be reduced through:

- Ventilation fans
- Waiting vehicles turned off
- PPE e.g.
    - Face masks
    - Hi-Visibility vests
- Shaded search areas
- Wind protection

Careful consideration of the risks and threats at a particular site will enable Security staff to design a well-planned search area

Volume of traffic

Understanding the amount of traffic expected to pass through the search area will determine:

- Number of search bays
- Use of bypass lanes for vehicles not required to be searched
- Layout of search bay approach, method of diverting selected vehicles

Type of traffic

Knowing what type of vehicles are going to need searching will determine:

- The physical space within the search bay
- The required area needed to turn vehicles around if rejecting search

9.3.2. Components of a vehicle search bay

Key information

A vehicle search bay is normally set up with the following components:

- Warning signs for approaching drivers
- Entry lane
- Entry point control barrier
- Search area
- Exit point control barrier
- Exit lane
- Driver holding area
- Prohibited items temporary storage area

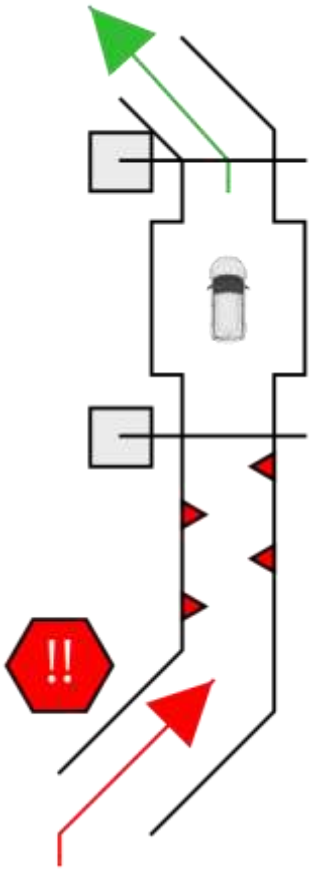


Figure 83 - example search bay components

9.3.3. Duty preparation and routines

Security staff coming on duty at a vehicle search bay should ensure that the required preparations have been completed. In addition to carrying the standard equipment required for security duty, a pre-duty checklist is a useful way to ensure that the searching activities will be successful.

Search bay pre-duty checklist	
Search equipment:	**Check**
Torch in working condition	✓
Under vehicle search mirror	✓
Gloves	✓
Prohibited items storage	✓
PPE:	✓
Hi-Visibility vest	✓
Sun hat	✓
Face mask	✓
Search bay layout:	✓
Search bay layout:	✓
Warning signs in position	✓
Entry lane walls in place	✓
Entry point barrier in place	✓
Exit point barrier in place	✓
Exit lane walls in place	✓
Driver holding area ready	✓
CCTV working	✓

Table 16 - Example pre-duty vehicle search checklist

Each site or search area may differ depending on the tools, technologies and nature of the search bay e.g. If it is a permanent structure, or temporary layout. Security staff will quickly become familiar with the requirements specific to the place of duty.

9.4. Vehicle search tools and equipment

A variety of tools and equipment are used to assist Security staff in searching vehicles, and correct use of these tools will increase the chances of detecting dangerous and prohibited items, or unauthorised removal of goods

9.4.1. Vehicle search tools

Common tools used to search vehicles include:

Mirror

- Used to search the underside of vehicles through observing the reflection
- May be equipped with a built in torch to light the underside of the vehicle
- May have wheels to assist with moving the mirror
- Extendable handle, and can be used to search on top of truck trailers or other high vehicles
- Only as effective as the operator – attention to detail and vigilance is essential

Figure 84 - Under vehicle search mirror

Torch

- Very useful for illuminating darkened spaces within a vehicle e.g.
    - Inside engine bay
    - Wheel arches
    - Behind hub caps
    - Internal storage

Figure 85 - Duty torch for vehicle search

Gloves

- Protect against injury when handling hot, sharp or jagged parts
- Reduce potential contamination of evidence

Figure 86 - Duty gloves

Traffic cones

- Guide approaching traffic toward the search bay entry lane
- Separate converging or diverging traffic

Figure 87 - Traffic cone

Lane barriers

- Force traffic to follow set path
- Block access to search bay
- Provide safety barrier for searching staff

Figure 88 - Traffic barriers

9.4.2. Vehicle search technologies

Examples of technology that may be used in a vehicle search bay includes:

Vehicle underside surveillance cameras

- Visual inspection of underside vehicles at high resolution
- Software analyses and compares scans against previous images of the same vehicle
- Can detect small changes to the underside of vehicles

Figure 89 - Under vehicle camera scanner

Complete vehicle x-ray

- Able to x-ray a vehicle providing an operator with images to analyse
- Can be used for large transport trucks

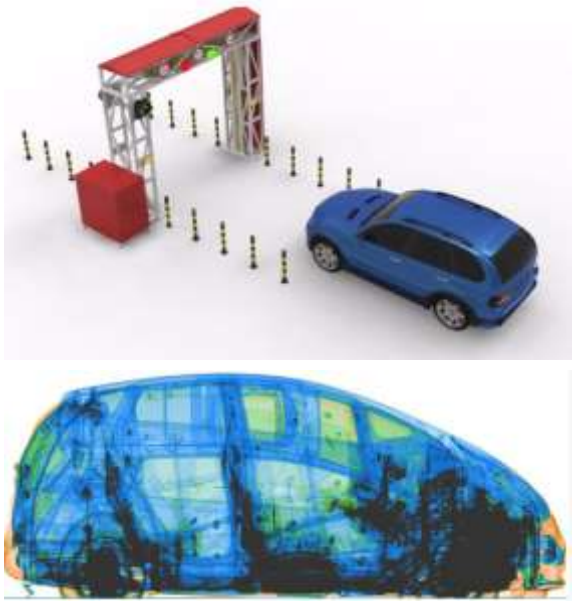


Figure 90 - Vehicle X-Ray

Explosive / Narcotics trace detector

- Machine detection of traces of explosive or narcotics
- Samples collected by swabbing surfaces of the vehicle
- Random or targeted screening of vehicles

Figure 91 - Handheld explosive trace detector

Figure 92 - Handheld narcotics trace detector

CCTV coverage (can be kept as evidence)

- Can provide additional eyes in the search bay
- Recording kept as evidence
- Safety of searcher and driver

The use of specific technology to assist in vehicle search will depend on the site and organisational requirements.

9.4.3. Use of canines for vehicle search

In particularly high threat locations, the use of dogs to aid in the search for dangerous or prohibited items can be very effective. Certain considerations must be made for the best use of search dogs including:

- Removal of drivers from the search area to reduce distraction of the dogs
- Rewarding the dogs with "False Finds" every shift
    - A search dog that doesn't find anything repeatedly will lose interest in the "game"
- Environmental conditions
    - Dogs can work for short periods only during hot conditions
- Cultural considerations
    - Some cultures may take offence at allowing a dog to search the interior of their vehicle

Figure 93 - Explosive detection dog working

9.5. Vehicle search procedures

The process of searching a vehicle can be broken into parts, resulting in a methodical and consistent approach to performing the task. This is key to successful search operations.

9.5.1. Directing vehicles into the search bay

When on duty as a Traffic controller, Security staff will need to keep in mind the following points:

- Effective communication with staff working inside the search bay
    - Radio/voice/visual contact
    - Relay update on search progress
- Control the rate of traffic entering the search bay lane
- Select vehicles according to site policy
- Give directions to drivers using the established hand signal procedures
- Remain vigilant to drivers actively avoiding search, and report as much detail as possible
- Identify potential indicators of threatening or criminal behaviour e.g.
    - Unusual vehicle appearance
    - Suspicious driver behaviour

Safety!

- At all times when working around moving vehicles, keep in mind movement patterns and safe spaces
- Comply with PPE requirements

9.5.2. Driver management

When working inside the vehicle search bay, Security staff must understand how to

approach, communicate and manage the drivers of vehicles. Whether the driver can remain in the vehicle during search, or be required to exit will be specified in the site vehicle search policy.

Reasons the driver may remain in the vehicle include:

- Low threat environment
- Search of cargo only
- Rate of search completions required
- Use of non-invasive technology in place of physical searches e.g. the under vehicle scanner and x-ray

Reasons the driver may be removed from the vehicle include:

- Need to conceal the search techniques from drivers
- High threat environment requires detailed searching
- Processing of driver documents at an access control point (concurrent activity)

Key information

Security staff should be very clear in communicating expectations to drivers to avoid confusion and potential conflicts. The following should be explained:

- Where to stop the vehicle
- When to leave the vehicle
- Where to move to once out of the vehicle
- Where to remain while the search is conducted
- When to return to the vehicle
- When to drive the vehicle out of the search bay

9.5.3. Conducting the vehicle search

The conduct of the vehicle search is critical, and failure to properly inspect could result in crime or safety threats going undetected.

Safety!

- Direct the driver to open internal storage compartments, bonnet, boot and fuel compartment. If there are any detonators, or booby traps linked to these areas, the driver may show hesitation in opening it themselves
- Never let a driver put their hands where they cannot be seen. They may be accessing a weapon, or removing prohibited items

Key information

The 10 areas to physically inspect when searching a light vehicle:

1. Underside
2. Driver and passenger areas inside the vehicle
3. Left front wheel arch, tyre and inner wheel assembly, side panelling
4. Hood and engine bay
5. Front bumper and light housings
6. Right front wheel arch, tyre and inner wheel assembly, side panelling
7. Right rear wheel arch, tyre and inner wheel assembly, side panelling
8. Trunk and spare tyre
9. Rear bumper and light housings
10. Left rear wheel arch, tyre and inner wheel assembly, side panelling

Note: Be sure to inspect any other place you identify that could be hiding something

Additional areas will be inspected for other vehicle classifications including:

Heavy vehicles

- Additional wheels and axles
- Tool bins fitted to the sides
- On the roof
- Air cylinders (braking systems)
- Luggage compartments of coaches
- Cargo hold of transport trucks

Specialist vehicles

- Buckets and scoops of earth moving machinery
- Under seat storage of forklifts and cranes
- Raised platform of scissor lift

Topic focus

A recommended process and sequence of inspecting the key areas is as follows:

- Start and finish at the same point of the vehicle every time
- Move in a clockwise direction around the vehicle
- Inspect each of the 10 areas from top to bottom
- Use a torch to clearly see internal spaces
- Move on to the next section only when satisfied that the current section is clear

If searching with a partner:

- Start at diagonally opposite sections of the vehicle
- Move in a clockwise direction
- Communicate with the partner when finished each section, and only move when both are finished with the current section – this avoids the feeling of pressure to move faster if being "chased" by a partner
- Finish at the same starting point

Searching with a partner can be very effective as it offers 2 sets of eyes on every section of the car.

Note: If a dangerous item is detected e.g. explosive or suspected explosive device, chemical hazard, or other dangerous material, the searcher should:

- Remain calm and make a quick mental note about
    - Location in the vehicle
    - Colours
    - Odours
    - Suspected material
- Evacuate the search bay to a safe distance
- Call the police and report the incident (Either directly, or through the control room)
- Detain the driver in accordance with the UAE Penal code related to the direct witnessing of a crime

Note: Prohibited items or goods must be processed as evidence, and Security staff should:

- Take photos of the items in the position found
- Confiscate the items taking care not to contaminate (wearing gloves)
- Record and document the items in accordance with the evidence handling procedures
- Secure the confiscated items and submit an incident report

Depending on the items detected, the police may also be called to deal with the driver and dispose of the prohibited items.

10 Areas of concern for vehicle search	
1. Underside **2.** Driver and passenger areas inside the vehicle **3.** Left front wheel arch, tyre and inner wheel assembly, side panelling **4.** Hood and engine bay **5.** Front bumper and light housings **6.** Right front wheel arch, tyre and inner wheel assembly, side panelling **7.** Right rear wheel arch, tyre and inner wheel assembly, side panelling **8.** Trunk and spare tyre **9.** Rear bumper and light housings **10.** Left rear wheel arch, tyre and inner wheel assembly, side panelling	

Module 9 Revision

Revision questions

1) Under what conditions are Security staff permitted to search a vehicle?

a) With consent from the driver

b) If the driver is acting suspicious

c) If the vehicle matches the site search policy

2) List 5 pieces of information to try to record if a driver refuses to have the vehicle searched

3) List 3 options security staff have when a driver has refused to be searched

4) Give 5 examples of information that will be found in a site vehicle search policy

5) List 6 of the 8 commonly used parts of a vehicle search bay e.g. entry lane.

6) Explain the sequence of searching a vehicle

7) Explain how to conduct a vehicle search when working with a partner

8) List the 10 areas of concern when searching a light vehicle

Module10
Person searching

Module 10

Person searching

Qualification Link

Units

- SEC03003NU18-Use security search methods and equipment

Learning outcomes

4. Interpret search policies and procedures
5. Select and use security search equipment
6. Search people

Key definitions

PPE – Personal Protective Equipment

Consent – the agreement given by a person who has been asked if they or their belongings can be searched

Screening – routine inspection of people and belongings passing through a screening point e.g. metal detector and x-ray

Screening point – the point of entry, exit or transition within a site where personnel are required to be searched

Physical search – inspection by using hands to search people or belongings

Visual search – visual inspection without physical contact

Self-search – display of items carried by presentation for visual search by Security staff

10.1. Personnel search regulations

Regulations related to the searching of people can be divided into 2 categories – UAE Law, and company policy. Security staff must be aware of both of these in order to confidently carry out their duties including the task of searching people and their belongings

10.1.1. Legal authority to perform searches

Security staff have the authority to perform searches of people and their belongings by consent only. This means that each person who is searched must be asked by the Security staff and must agree to the search.

Key information

Some organisations may require that staff and visitors are searched prior to entry or exit from the premises. This will often be in the form of a walkthrough metal detector, and possibly x-ray scanning of their bags or belongings. In cases such as this, the consent is given by individuals as a condition of employment by the company or entry to the premises. If a more detailed physical search is required, individual consent must be confirmed beforehand.

If a detailed physical search is required in any unusual or unplanned circumstances, Security staff should ask the person to be searched to sign a note of consent in the official security notebook, or a purpose designed consent form.

It should be noted, that if a person refuses to be searched, or proceed through normal screening procedures e.g. metal detector and x-ray, the Security staff can take further steps to ensure safety and security including:

- Deny access to the site or facility
- Report the refusal to management or the police
- Detain the person refusing to be searched based on evidence supporting a crime has been committed

10.1.2. Searching of females

UAE Law requires that only a female will search another female or her belongings. If a detailed physical search is required, Security staff must be prepared to arrange for a female member of staff to perform this search

Key information

Females may pass through normal screening points in view of the general public, however for any detailed physical searches, a private area

must be used

10.2. Personnel search policies

Organisations will work together with Security managers to develop personnel search policies applicable to the organisation or site.

10.2.1. Aims and purpose of personnel searching

The aim of searching personnel at a site or facility is to protect people, property and information through controlling what is carried through security checkpoints and into a site. The reasons for conducting personnel search may be many, however common reasons include:

- Preventing prohibited or dangerous items from entering a site
- Detecting theft or unauthorised removal of items from a site
- Locating evidence to confirm suspicions of a crime

10.2.2. Who needs to be searched

According to the organisational policy, and depending on the threats and risks to the site the following may need to be searched:

- Visitors
- Permanent employees
- Hand carried baggage
    - Suitcases
    - Laptop bags
    - Backpacks
    - Toolboxes
    - Handbags and purses
- Contractors
- Delivery drivers
- Everyone (100% of personnel at a site)

10.2.3. Personnel search policy contents

Search policies will be different depending on the organisation and threat level, however the basic structure of a personnel search policy will remain similar and will usually specify:

- Prohibited items to be detected
- Who needs to be searched
- Search level of detail, depending on;
    - Threat levels
    - Volume of traffic
    - Technologies utilised for search
    - Public perception
- Selection criteria
    - Percent of persons to be searched
    - Visitors
    - Employee
    - Contractor

The development and implementation of effective personnel search policies is the responsibility of the organisational management and Security managers, however Security staff must be able to interpret the requirements and apply the policies with confidence in order to contribute to the safety and security of the organisation

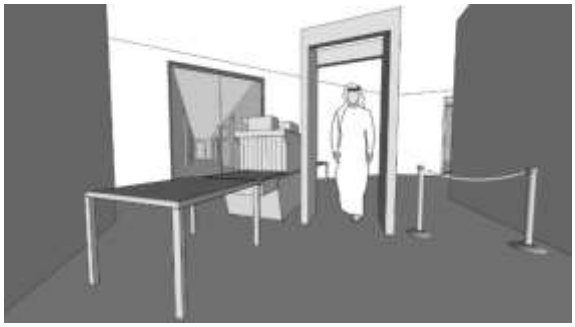


Figure 94 - Security screening point

10.3. Personnel search area set up

Security staff will be expected to ensure that the area to be used for the searching and screening of personnel is set up and ready to use in accordance with the site policy and procedures

10.3.1. Parts of a personnel search area

Screening points may be different in design according to the requirements of a particular site or organisation, however some common components of a screening point include:

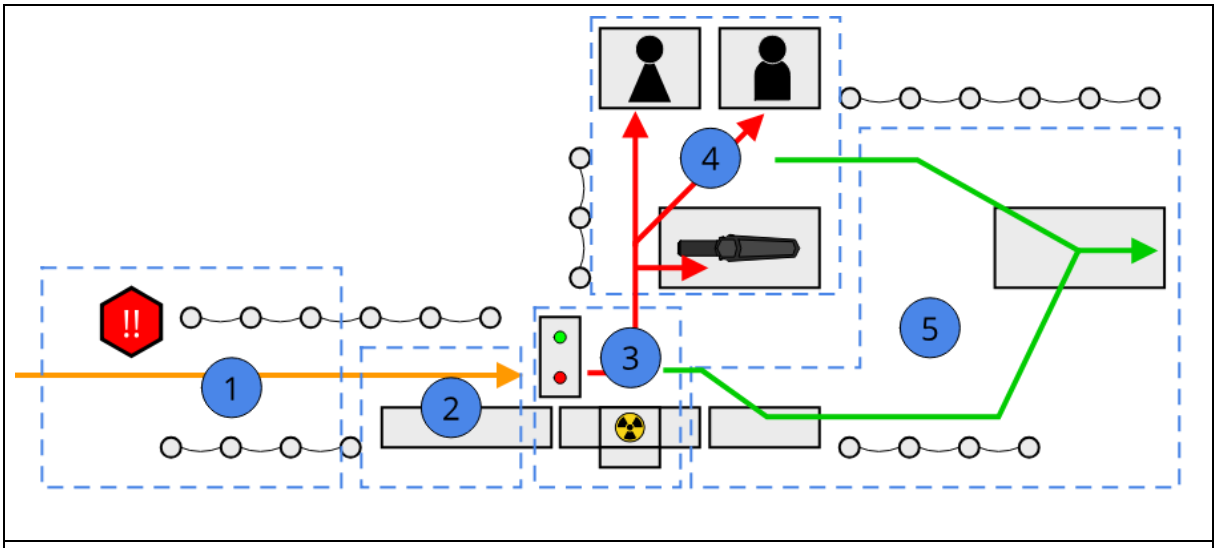
1) Pre-screening & queue zone
2) Unpacking area
3) Search zone
4) Follow up search area
5) Repacking and exit zone

Understanding these 5 primary components of a screening point will assist Security staff in ensuring a smooth transition of personnel through a screening point, and maintenance of control and order during the searching process

10.3.2. Layout of a personnel search area

The physical placement of search point components and equipment will require some consideration of a variety of factors present at the site or facility, including:

- The level of discretion required by the organisation (open and obvious, or low profile)
- Physical space available
- The placement of security access zone transition points
- The equipment and technologies used
- Staff available to operate the screening point
- Number of personnel expected through the screening point



1) Pre-screening & queue zone
2) Unpacking area
3) Search zone
4) Follow up search area
5) Repacking and exit zone

Figure 95 - Example personnel search layout

Key information

Knowledge of these screening point factors will assist in developing a screening point layout that will achieve the most desirable performance including:

- Complete control of all movements through the screening point
- Rapid processing times
- Enhanced detection probability
- Reducing stress of persons being searched

In order to achieve these outcomes, Security staff should if possible:

- Give people plenty of warning that a security screening point is ahead
- Split queues to reduce perceived waiting time
- Use ropes or gates to funnel personnel through the search zone
- Use enough staff to support follow up searches, without compromising the initial search flow
- Use access control systems to progress screened people out of the screening point e.g.
    - Automated gates
    - Turnstiles

10.3.3. Segregated search areas

A screening point should include segregated areas to conduct search of females, or to carry out follow up searches if any initial search has indicated that further investigation is required.

Key information

Segregated search areas for the physical search

of Females must be away from public view and CCTV coverage

Space should be allocated within the search zone to conduct more detailed screening without having to go to another area e.g.

- to conduct spot searches using a hand held metal detector.
- To carry out a physical inspection of a person

Key information

A separate room or enclosed area can be used if the search requires the removal of items of clothing, or cultural or religious garments.

10.4. Tools for searching people

Security staff will be expected to use a variety of tools and technologies to assist with searching people and belongings and increasing the rate of detection

10.4.1. Tools and technologies overview

There is a wide range of tools and technologies available, and their use at a site or organisation will depend on the risks, threats, type of organisation and who is passing through. The most commonly used tools include:

- Walk-through metal detector
- Hand held metal detector
- Baggage X-Ray
- Particle detectors (Explosives, narcotics, chemicals)

More advanced technologies that are in use at some high risk locations e.g. Airports:

- Person scanning X-Ray
- Person thermal scanning (Detection of infectious viruses)

10.4.2. Handheld metal detector operation

One of the most basic search tools that Security staff will use is the handheld metal detector. This device is used to precisely locate any metal object carried by a person, allowing Security staff to identify the object and determine if it presents a risk or not.

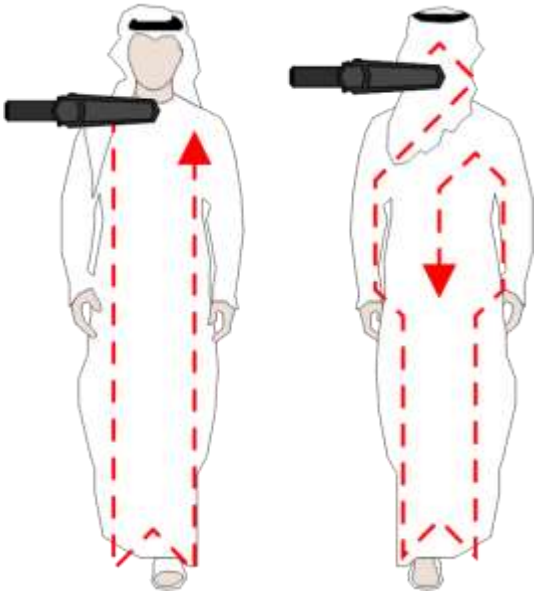
A handheld metal detector uses a magnetic field generated by transmitter and receiver wire coils built into the detection surface. Disruptions to this magnetic field are caused by metallic objects and are therefore able to be detected.

Topic focus

To use the handheld metal detector:

- Turn the device on
- Move the device across the recommended search pattern
- Give special attention to;
  - The waist
  - Under the arms
  - Ankles
  - Pocket areas

Recommended Search Pattern



Front side **Back side**

Detection capabilities

High performance handheld metal detectors can provide detection of these examples:

- Pistol – 22cm distance
- Knife – 15cm distance
- Razor blade – 7cm distance
- Foil wrapping – 3cm distance
- Small jewellery – 3cm distance

Note 1: Most metal detectors can be switched

to silent, and a warning light or vibration replaces the detection alarm – useful for more discrete searches

Note 2: The temporary push button can be used to eliminate interference from nearby metal objects such as reinforcement in concrete structures or metal walls

Key information

Handheld metal detectors are battery powered, and care should be given to the condition of the batteries. Security staff must check:

- Battery connection points are free of rust or corrosion
- Recharging works correctly

Defects should be reported for maintenance, and a correctly working device taken on duty

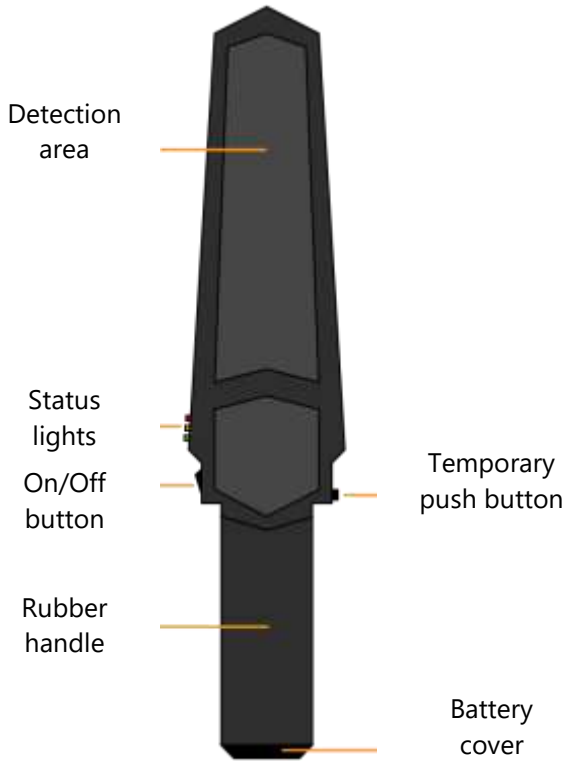


Figure 96 - Handheld metal detector parts

10.4.3. Walkthrough metal detector operation

The use of a walkthrough metal detector is common in many places requiring 100% screening of personnel within the site. Security staff must understand how to operate a walkthrough metal detector device, and its limitations in order to ensure the safety and security of a site.

Common features of a walkthrough metal detector include:

- Stop/Proceed indicator lights
- Zone detection
- Sensitivity adjustment
- Totals counter

Topic focus

Security staff must be capable of operating the walkthrough metal detector, and this process can be broken into **2 parts.**

Part 1 - Start of duty inspection:

- Check power cables in good condition and protected from foot traffic
- Verify detection of metallic objects through all zones using a test item
- Verify status lights working (stop & proceed)
- Reset the scan counter (organisation may require search count data)

Part 2 - Normal screening operations

- Stand in a position on the "Safe" side of the screening point where clear communication with entering personnel can be achieved
- Coordinate the flow of personnel through the metal detector
    - Ensure personnel have placed any metallic objects in a belongings tray before passing through
    - Ensure personnel only pass through when the device is indicating "Proceed"
- Observe for any detections indicated by the device (Alarm sound, and zone detected light)
- If a detection is made;
    - Request the person to self-inspect the area and ensure no metallic objects are carried
    - Send the person through the device again to verify the detection
- Upon secondary detection from the walkthrough metal detector, direct individuals to a follow up search zone to one side of the screening point
- Upon identification of prohibited and dangerous items, process in accordance

with site and organisational policies and procedures

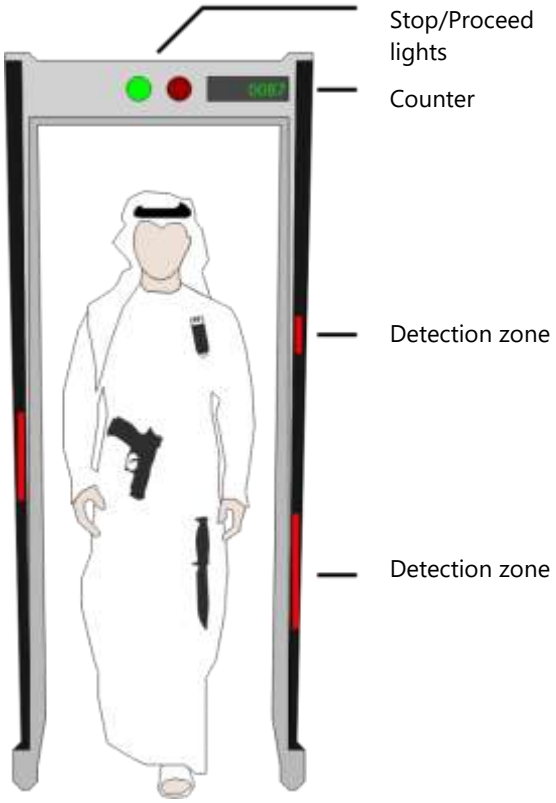


Figure 97 – Example walkthrough metal detector components

10.4.4. Baggage X-ray operation

Using an X-Ray machine to scan bags and containers is a very effective method of detecting prohibited and dangerous items. X-Ray equipment is commonly used at screening points within:

- Ports, Airports and Border control points
- Government buildings
- Tourist attractions
- Military camps

Security staff may be required to operate an x-ray scanner to support security searches, and the basic principles of operating this equipment should be familiar

Safety!

- X-Rays are a form of ionising radiation, which means that accumulated exposure may cause health risks. Do not operate and X-Ray machine without the protective lead curtain in place
- When the X-Ray machine is powered on, do not insert any body parts or animals through the tunnel

The features and capabilities of an X-Ray machine will vary depending on the model and manufacturer, and Security staff are encouraged to read the original equipment instructions provided with the X-Ray machine.

Topic focus

Basic operation of the X-Ray machine

The operation of an X-Ray machine can be described in 5 parts

- Machine inspection
- Powering on the machine
- Operating the machine
- Inspecting Objects
- Powering off the machine

Part 1 – Machine inspection:

- Confirm power voltage required and ensure power cable is properly connected
- Check all emergency stop buttons are in the 'Reset' position
- Do not start the machine if any emergency stop buttons are not working
- Check the lead curtains at tunnel entry and exit have no gaps or damage
- Check the conveyor belt for cracks, damage or misalignment
- Check inside the tunnel for any objects left inside
- Report any issues identified to the shift supervisor and prepare a maintenance request

Part 2 – Powering on the machine

- Insert the key into the switch on the control keyboard and rotate to 'ON'
- Press and hold the power button until the power light comes on

Part 3 – Operating the machine

- Wait for the machine to pre-heat
    - Depending on the machine, and how long since last use it may take 1-20 minutes to pre-heat
- Log in to the system using the user profiles as required
- The machine can now be controlled using the keyboard
- Progress the conveyer belt to confirm correct operation

Part 4 – Inspecting Objects

- Place the object or bag on the conveyor belt at the tunnel entry
- Click on the move button to run the conveyor belt forward and backward as necessary
- When the objects are scanned, the X-Ray lights will light up, and the scanned image will be displayed
- The image can now be inspected for prohibited or dangerous items (more details on interpreting images are given in the next section)
- When the object arrives at the tunnel exit, press the conveyor stop button and remove the object.
- The X-Ray operator can now proceed to the next item to inspect

Part 5 – Powering off the machine

- Check the conveyor belt for any objects remaining, if any found, remove and inform the shift supervisor
- Press the stop button and rotate the key switch counter clockwise to the 'OFF' position
- Remove the key from the key switch and secure it in accordance with site key storage policy

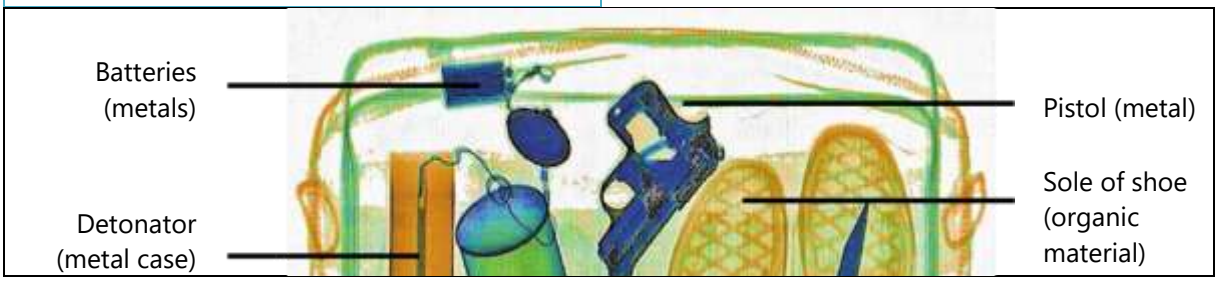
Key information

The standard colours used for X-Ray image display are:

- **Blue** – Hard materials including metal, hard plastic, wires, batteries etc.
- **Orange** – Organic materials including rubber, leather, food, explosives, liquids, gels, and powders
- **Green** – Light plastic, soft metal alloy

Note 1: Objects that are very light, thin, dirty or damaged should be placed in a plastic tray and sent through the tunnel for inspection

Note 2: Electronics can be separated from other baggage for individual inspection, as the X-Ray images will be very complex and this will allow for a clearer inspection of the internal components of any electronic devices



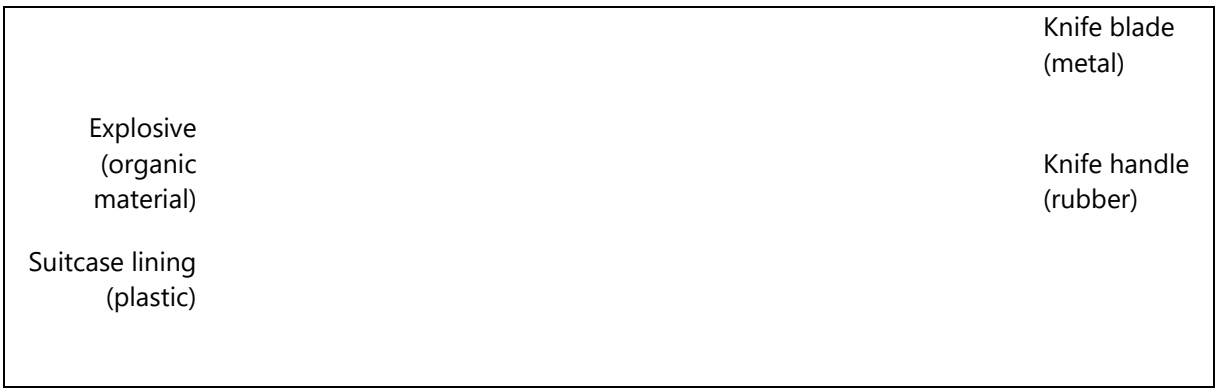


Figure 98 - Example X-Ray image interpretation

Image analysis

In order to better view and analyse X-Ray images, operators can use the following common functions of the X-Ray machine to enhance the scanned images and interpret the contents of the items

Button	Function
Colour/Black and white	Switch between colour image, and black and white image
Organic Exclusion mode	Turns all biological material grey, allowing remaining material to be seen in colour (e.g. metal guns, knives etc.)
Non-Organic Exclusion mode	Turns all non-organic material grey, allowing remaining material to be seen in colour (e.g. drugs, explosives, liquids)
Magnification	Zoomed image for close inspection of contents
Suspicious organic enhancement	Highlights certain objects on the screen according to their content e.g. ▪ Water, plastic explosives ▪ Impure drugs or homemade explosives ▪ Pure drugs
Edge enhancement	This allows the image to be sharpened, with object edges enhanced

Table 17 - X-Ray image interpretation functions

Detection of suspicious items

If analysis of an X-Ray image reveals a suspicious item, Security staff must further investigate and may carry out a physical search of the item to confirm the contents. Procedures for this action are described in a later section.

10.4.5. Use of canines for personnel search

A highly effective tool for assisting in the search of personnel and their belongings is the use of trained dogs. Dogs can be trained to effectively detect:

- Explosives
- Narcotics
- Cash
- Organic materials (Food, plants etc.)

Canine detection methods may be used at Airports, Ports, National borders, military camps and other high risk locations.

Benefits to be gained when using Canines for security searches include:

- High volume of personnel can be screened by a single search dog, rapidly and reliably for the materials in which the dog is trained to detect
- Many bags and items can be searched quickly and effectively
- Visual presence of search dogs acts as a strong deterrent to potential criminals

The use of dogs for searching presents several challenges including:

- **Public perception**
  - Search dogs can be viewed as very confronting, and in invasion of personal space

- Presents an image of 'high security' alert
- Certain dog breeds convey feelings of fear or apprehension

- **Working conditions**
  - Weather, and environment can affect the performance of search dogs
  - Volume of personnel to be searched can cause fatigue in search dogs
- **Maintenance and housekeeping**
  - Require housing, cleaning and grooming
  - Require continuation training

Security staff on duty at a place that uses canines for personnel search must be aware of the impacts that such a security operation can have, and must follow guidance given by the dog handlers.

10.5. Personnel search procedures

Each site or organisation may have developed specific search procedures, however the basic principles of conducting a personnel search will remain the same.

10.5.1. Controlling the rate of searches

When working at a site that is required to conduct a large amount of searches on people entering and exiting, controlling the rate is essential to maintaining safety and security.

Security staff on duty at a screening point will need to:

- Maintain order in the pre-screening and queue zone
- Direct individuals to move forward when the previous person has been searched
- Prevent uncontrolled advancement through the screening point

Failure to control this area will increase the risk of personnel passing through the screening point in possession of prohibited or dangerous items, and add to confusion in a busy working environment

10.5.2. Giving direction to personnel to be searched

When communicating with personnel in a security screening point, Security staff should:

- Make comfortable eye contact with each person
- Use clear and simple directions
- Maintain courtesy and respect for each person
- Be firm and professional at all times

At some sites or organisations, many of the permanent employees or regular visitors may know the established search procedures and will pass through the screening point smoothly, however, there may be others who are unfamiliar with the site and procedures and clear direction and control by Security staff is essential

10.5.3. Applying search techniques

Safety!

When preparing to search any person or item by hand, the appropriate PPE must be worn depending on threat and risk e.g.

- Protective gloves (sharp needles, blades etc.)
- Latex gloves (Infection, contamination etc.)

Search tools and technologies are valuable in assisting detection of prohibited items and materials, however a physical search done with the hands is an important skill for Security staff. Applying physical searching techniques in a safe and thorough way can increase detection and confirm the presence of prohibited and suspicious items

10.5.3.1. Physical body search

Topic focus

The physical body searching process can be divided into 2 steps

Step 1: Prepare to search

- Gain consent of the person to be searched
- Assess the location in which the search will

be conducted e.g.
    - Private room
    - In public location
- Wear appropriate PPE
- Give clear and professional directions to the person being searched

Step 2: Perform the search

Using hands, physically inspect the 8 zones of concern:

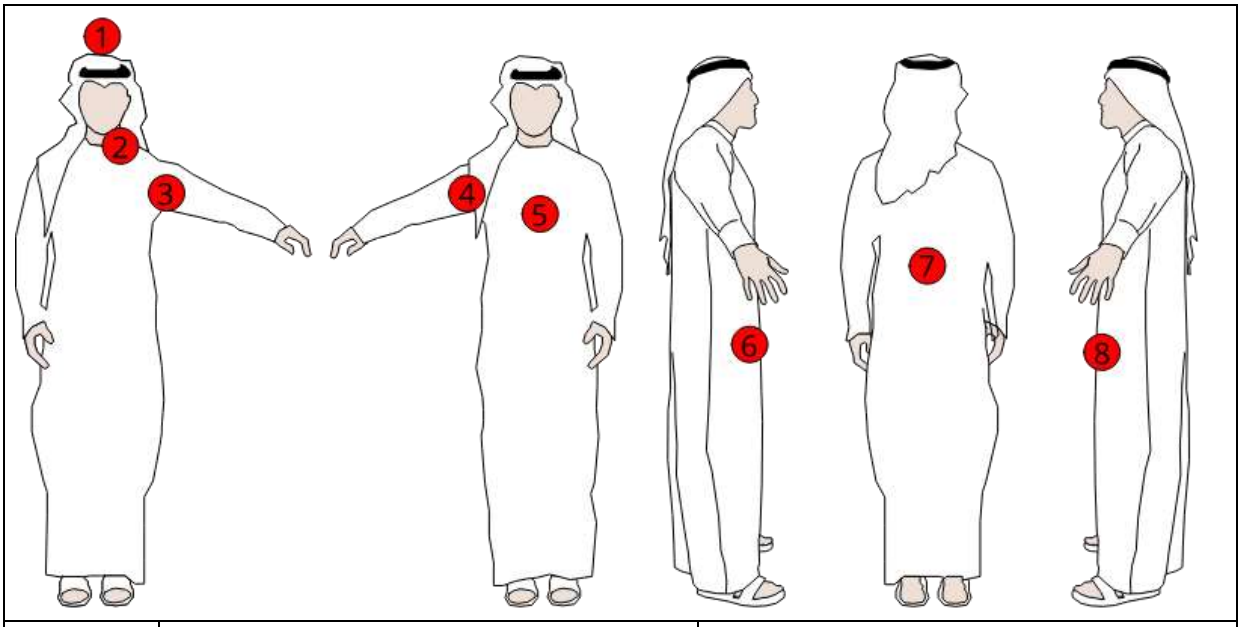
1. **Head, hair and headwear**
2. **Collar**
    2.1. Turn the collar up
    2.2. Roll the fabric checking for sewn in items
3. **Right arm**
    3.1. Direct the person to extend the whole arm
    3.2. With both hands pat from the armpit outward to the wrists
4. **Left arm**
    4.1. Direct the person to extend the whole arm
    4.2. With both hands pat from the armpit outward to the wrists
5. **Front of torso and waist**
    5.1. Pat the torso from top to waist
    5.2. Inspect shirt pocket linings
    5.3. Inspect shirt seams
6. **Right groin, leg, ankle and foot**
    6.1. Stand to the right of the person
    6.2. With both hands pat the inner and outer thigh
    6.3. Pull trouser pockets inside out
    6.4. With both hands pat the leg down to the ankle
    6.5. Lift trouser hem and inspect ankles and socks
    6.6. Remove shoes and inspect insole, tongue and laces
7. **Back of torso and waist**
    7.1. Pat the torso from neck down to waist
    7.2. Inspect shirt seams
8. **Left groin, leg, ankle and foot**
    8.1. Stand to the left of the person
    8.2. With both hands pat the inner and outer thigh
    8.3. Pull trouser pockets inside out
    8.4. With both hands pat the leg down to the ankle
    8.5. Lift trouser hem and inspect ankles and socks
    8.6. Remove shoes and inspect insole, tongue and laces

Note 1: This procedure is the most complete physical search. Security staff may use only some of these techniques depending on the site, threat and organisational requirements

Note 2: Deliberate movements and methodical process will send a message of professionalism and thoroughness rather than personal intrusion

Key information

If the person to be searched is wearing a head covering of cultural or religious significance, it may be very offensive to remove this in public. Consideration should be given, and if required the search conducted in a private location



	1. Head, hair and headwear **2.** Collar **3.** Right arm **4.** Left arm	**5.** Front torso and waist **6.** Left groin, leg, ankle and foot **7.** Back of torso and waist **8.** Right groin, leg, ankle and foot

Table 18 - Physical body search procedure

10.5.3.2. Physical item search

Security staff may be required to inspect the contents of personal belongings such as:

- Purses and handbags
- Backpacks
- Laptop bags
- Tool boxes
- Suitcases

Topic focus

If Security staff suspect dangerous or prohibited items are hidden within the personal belongings of a person, a physical search can be divided into 2 steps:

Step 1: Preparing to search

- Gain consent from the owner of the belongings
- Separate the item (bag, case, box etc.) from the primary search area
- Direct the owner to place the item on a secondary search table

Step 2: Performing the search

- Direct the owner to open the item
- Visually inspect the contents (do not touch anything)
- Direct the owner to remove items of interest and place them on the table for closer visual inspection

Note 1: This method of directing the item owner to physically handle and present suspicious items to Security staff will reduce the risk of contaminating potential evidence, and any claims of damage caused to personal items during the search

Experience and practice will enable Security staff to quickly identify occasions where a physical search of items is required, and perform these searches efficiently and safely.

10.5.4. Searching people outside of a designated search area

The nature of security operations is such that things will often happen unexpectedly. There may be times where Security staff need to perform a physical search of personnel or their belongings outside of a purpose designed security screening point.

Considerations to be made when deciding to search at other locations within a site include:

Evidence of consent

- Ask the person to sign a statement in the official notebook giving consent for the search
- Obtain a witness if possible

Personal safety

- Choose a well-lit location
- Move away from any traffic hazards
- Request back up Security staff if available
- Communicate the intent to perform a search with the control room
- Choose to perform the search under CCTV coverage if available

10.5.5. Handling search refusals

Individuals are within their rights to refuse to be searched by Private Security staff, and if this occurs, Security staff must be prepared to deal with this situation.

Key information

Options available to security staff in the event of a refusal to be searched include:

- Deny access to the site or area
- Record personal details of the person refusing search
- Report the occurrence to supervisor
- Call the police

Security staff should always attempt to gather as much information as possible about the person and circumstances around the search refusal

The circumstances under which the search is refused will guide Security staff in making the proper decision, and standard operating procedures SOPs will clearly describe the procedure to be followed for escalation to management

10.6. Handling prohibited items

A successful detection of prohibited items by security staff will require proper handling and storage of the items that have been found. Procedures for this may be different depending on the site, organisation and legal requirements, however the basic approach will remain the same

10.6.1. Identifying prohibited and dangerous items

In order to identify prohibited and dangerous items, Security staff must be familiar with site duty instructions that list what is not permitted to be brought on and off a site. Further to this, an awareness of what could cause damage or harm will help in identifying other dangerous items and substances when conducting security searches

Common examples of prohibited items may include:

Airports

- Flammable gases, liquids and gels
- Weapons
- Food items
- Etc.

National borders

- Untaxed goods
- Drugs/Alcohol
- Plants and animals
- Large amounts of cash

Construction sites

- Unauthorised removal of construction materials
- Cameras and recording devices

Corporate headquarters

- Removable media storage (USB, Hard drive etc.)
- Weapons
- Unauthorised removal of printed documents

This list is an example of the type of items and materials that Security staff will need to detect during security screening activities, and a thorough knowledge of site specific requirements will enable the safety and security of the organisation

10.6.2. Processing prohibited and dangerous items

Any item that is detected by Security staff, and is determined to be prohibited, may be confiscated and stored by the Security team as evidence.

Safety!

Be aware of risks presented by prohibited and dangerous items including:

- Sharp edges
- Explosive potential
- Chemical exposure
- Biological contamination or infection

Before physical handling any item, PPE must be worn

Topic focus

Processing prohibited and dangerous items

When confiscating prohibited items, Security staff must follow the rules of evidence handling as previously described:

- **Collection**
  - Wear gloves to prevent contamination of the evidence
  - If more than one item of evidence is collected, change gloves in order to maintain a sterile connection to the evidence
  - If evidence is a substance, collect a sample on a sterile swab and place into a zip lock bag
- **Securing**
  - Prevent any further access to the item of evidence
- **Preservation**
  - Keep the evidence in an appropriate environment to preserve the usefulness at a later time
- **Identification**
  - Label the evidence bag with Company name, Staff name, date, time, location and evidence number
- **Continuity of custody**
  - Ensure a record is kept of the transfer of evidence from one person to another
- **Logging**
  - Document all items of evidence in an evidence register

Handling of dangerous items

Any items detected that present an immediate threat to health and safety must be handled by the relevant authorities. For example:

Explosives/Chemicals/Biohazard detected

- Call the police
- Evacuate the area
- Lock down access to the area (Cordon and control)

Module 10 Revision

Revision questions

1) According to UAE law, private security staff must receive consent before searching people or their belongings?

TRUE / FALSE

2) Who can search females?

a) Any member of the security team
b) Another female only
c) Male police

3) List 3 pieces of equipment to help searching people

4) List the 5 zones commonly used to lay out a security screening point

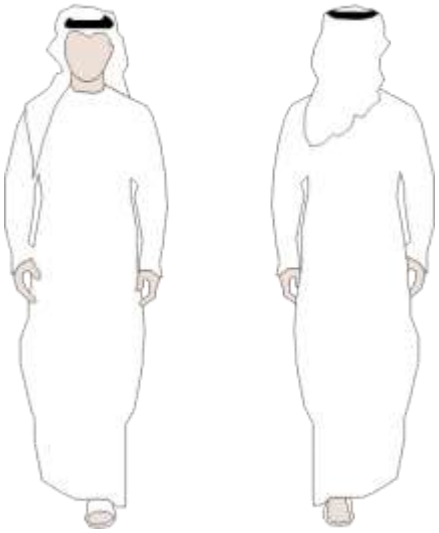
5) Identify the types of material associated with each colour on an X-Ray image

Blue -

Green -

Orange -

6) Draw the recommended search pattern when using a hand held metal detector



7) List 3 pre-duty inspection items to check on the Walk through metal detector

8) Which side of a Walk through metal detector should Security staff stand?

a) Entry side
b) Exit side
c) Directly to the side

9) List the 8 areas to inspect when conducting a physical body search

10) List 3 considerations to make when searching a person outside of a purpose designed screening point

11) List 4 items that Canines can be trained to detect

12) How should prohibited items be handled when detected during a security search?

a) According to the 6 steps of evidence handling
b) Thrown into a prohibited items bin
c) Placed in a pocket to hand over at the end of shift

Module 3

Access Control

Module 11

Access control

Qualification Link

Units

- SEC03002NU18-Carry out site access control procedures

Learning outcomes

1. Interpret access control procedures used at an entry or exit control point
2. Conduct entry and exit control procedures
3. Use access control systems at a security control point

Key definitions

Access control – a system or method used to determine who is allowed to enter an area

Entry control – a physical barrier used to control transit through a secure zone

ACP – Access control point

RFID – Radio frequency identification

11.1. Aims and purpose of access control

Access control is a fundamental principle of security a site, property or organisation. There are many methods of controlling access, and levels of implementation, however the basic principles of this security measure will remain the same.

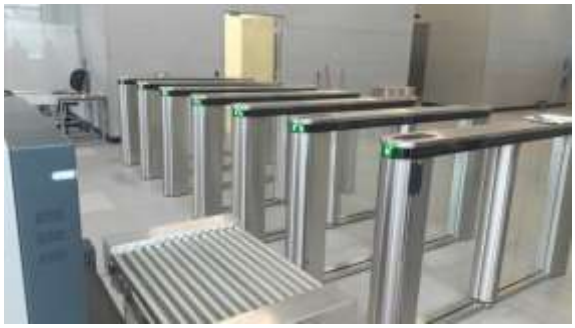


Figure 99 - Turnstiles used to control access

11.1.1. Purpose of controlling access at a site

Key information

Access control points may vary in size and complexity, but the main purpose is to provide an organised structure and method for allowing authorised people or vehicles to pass smoothly, while denying access to unauthorised people or vehicles. This allows an organisation to:

- Reduce the risk of criminal or damaging behaviours
- Monitor the type and quantity of people or vehicles accessing certain zones
- Account for people and vehicles location at all times
- Increase safety and security within a site

11.1.2. Principles of access control

Topic focus

There are 3 basic principles of any access control system:

- **Access permission**
  - Who?
  - Where?
  - When?
- **Identity verification**
  - Positive ID
  - Legitimate holder
- **Controlled entry**
  - Barriers opened
  - Progression permitted

How these principles are applied to a site, zone or critical area will depend on the threats, risks and organisational requirements.

A very simple example of an access control system would be the use of an electronic lock on a single door, with key card access. Reviewing the 3 basic principles it would look like this:

- **Access permission** – The key card is issued to an authorised person
- **Identify verification** – the card reader recognises the signal emitted by the key card as correct for that location
- **Controlled entry** – Electronic lock releases

allowing the key card holder to pass through

An example of a more complex system of access control would be at the main entrance to a busy industrial site, with a large range of people, vehicles and materials requiring access to different parts of the site. The application of the access control principles will need to be carefully planned in order to handle such a complicated security environment

Security staff will quickly learn to recognise how the basic principles of access control are used at their place of duty.

11.2. Access control policies

Organisational leadership and Security managers will work together to develop suitable access control policies for specific sites and locations, and Security staff will need to become very familiar with these policies in order to work effectively at an access control point

11.2.1. Using site access control policy

Security staff working at an access control point will refer to the approved access control policy, and the information contained within this document including:

- How site users are categorised e.g. visitor, employee etc.
- Permission levels granted to category of site user
- Identification requirements
- Progression routes through the access control point
- Access logging requirements
- Incident escalation procedures

Key information

Security staff must ensure that the current approved policies are followed, and a copy will be kept at the access control point, and in the security control room.

11.3. Access control roles and responsibilities

Security staff working at an access control point may be required to perform multiple roles and duties, and the size and design of the access control point may mean that some roles are not required, or there are multiple staff working in the same role. It is important to note that some of the roles described can be performed by technologies available, however it is vital that Security staff are competent at performing these tasks manually

11.3.1. Movement controller

The movement controller is responsible for progressing site users forward into the access control zone, and duties will include:

- Controlling the flow of people or vehicles into the ACP
- Pre-screening of site users, directing different categories of user to the appropriate area within the access control zone
- Maintaining order at the approaches to the ACP
- Identification and early detection of possible security threats

At some sites this role could be performed by technologies such as stop/go lights, or even achieved through clear signposting and instructions to approaching site users

11.3.2. Access controller

The access controller is responsible for identifying the category of site user, verifying identity and applying the permissions specified within the approved access control policy. Specific duties will include:

- Inspecting ID
- Verifying access permission including;
    - Visitor pre-approval lists
    - Contractor work orders
    - Staff access permission
    - Delivery confirmation
- Issuing badges and passes
- Logging details of site users granted entry
- Organising escorts as required

This role is certainly performed by technology at many sites and at ACP's that are not manned

by physical Security staff. The technologies used for this task will be explained in a later section.

11.3.3. Escort

The security escort is responsible for guiding and monitoring site users who do not have the access permission to move freely within a secure zone. Duties include:

- Direct supervision of visitor movements
- Monitoring of actions and activities carried out by contractors or maintenance teams
- Communication with the security control room on location and movements
- Returning visitors and other unauthorised site users to the ACP for outward processing

11.3.4. Entry control point supervisor

The entry control point supervisor is responsible for the overall security effort at the ACP, and duties include:

- Coordinating the rotation of duties within the ACP
- Ensuring staff enforce the access control policy correctly
- Resolving complex access issues
- Preparing incident reports

11.4. Access control tools and technologies

In addition to a physically staffed ACP, access to security controlled zones can be achieved or enhanced through a variety of tools and technologies. These can be categorised as either:

- Mechanical
- Electronic

These 2 methods of controlling access can be combined, and also deployed in support of Security staff manning an ACP

11.4.1. Mechanical access control

Mechanical access control is normally described as the locks and barriers that require manual movements to open.

Mechanical access control examples include:

- Manually operated barrier arm
- Remote operated barrier arm
- Chain or rope
- Sliding gate
- Lock and key
- Combination lock
- Deadbolt
- Physically supervised door

There are many forms that each of these examples may take, however the main feature of mechanical access control is that it requires operation by a person

Manual barrier

Chain barrier

Sliding gate

Remote barrier

Figure 100 - Mechanical access control options

Safety!

- Any mechanical equipment that is used to control access must be inspected for damage and wear. Security staff will need to conduct scheduled checks on the condition of barriers, chains, locks and gates.
- When operating mechanical access control equipment, remain aware of pinch and crush points, keeping fingers, hands and limbs clear of danger.

11.4.2. Electronic access control

There are many electronic access control systems available in the security industry, and multiple ways in which they may be implemented and integrated.

Key information

Typical features of an electronic access control

system include:

- **Identity management** (database of who, where and when access is authorised)
- **Encoding of ID credentials**
- **Reading of ID credentials**
- **Granting of access** (authorisation checked at remote database)
- **Recording entries and exits to a database**

These features are very attractive to many organisations as they can be used to support other operational functions such as:

- Attendance management
- Cancelling of access privileges
- Accounting of personnel in emergency situations e.g. fire evacuation

Electronic access technologies can also be integrated for monitoring within a security control room, adding flexibility to the security operations at a site or organisation.

Topic focus

Electronic access control technologies can be divided into several categories

Figure 101 - RFID card and reader

RFID - This technology is most commonly used in the security industry as a 'Key card' access system. Features of this technology include:

- Vicinity reading (6-10m reading distance)
- Proximity reading (approx. 10cm distance)
- No personal details stored in the card, only a number that references a remote database

Strength:

- Simple to issue and carry
- Rapid logging of user location, time etc.

Weakness:

- Vulnerable to theft
- No verification of authorised owner using the card

Figure 102 - Passcode access keypad

Passcode – This can take the form of a PIN or phrase used to verify identity on a keypad

- User defined passcode
- Stored in a control panel or database

Strength:

- Only the user will know their passcode
- Less vulnerable to theft

Weakness:

- Can be shared by dishonest users
- May be guessed by others

Figure 103 - Fingerprint reader

Biometric – Reading of a person's biometric information such as fingerprint, voice or retina pattern

- Unique to each individual

- Personally identifiable data stored in a database
- Useful for personnel entry points

Strength:

- High level of security
- Difficult to falsify biometric readings

Weakness:

- May be costly to install and manage

Figure 104 - Iris and fingerprint scanning unit

There are many variations of these technologies, and are often combined within a site at different locations depending on the security requirement.

Each method of electronic access control carries strengths and weaknesses, and Security staff should be aware of how such a system may be compromised by potential criminals.

Vigilance is always required by Security staff, even when the most sophisticated electronic access control system is installed, as criminals will always look for a way to exploit the system.

11.5. Controlling movement at an access control point

The physical movement of people and vehicles through an ACP should be controlled in such a way that Security staff capable of methodically processing each potential site user in an efficient and coordinated way. The factors that determine how an ACP will flow depend on the design, assisting technologies, types and number of site users, and staff available.

11.5.1. Access control point design

Security staff may not be directly responsible for the design and layout of an ACP, however a thorough understanding of the design considerations will assist Security staff in operating the ACP to its highest potential. The design of an ACP will always depend on the specific requirements of the site or organisation, however a best practice for high risk sites can be learned, and Security staff can then choose to apply the levels as appropriate to the place of duty.

Key information

The ideal design for a significant ACP for a site or building will include three specific zones:

- **Approach zone**
- **Access control zone**
- **Response zone**

Careful planning of the layout of these zones will provide Security staff with the best opportunity to Detect, delay and respond to unauthorised access attempts

Note: An ACP must have in place methods to prevent the circumvention of the ACP e.g. walls, fences, landscaping or other features requiring a potential site user to pass through the ACP

11.5.1.1. The approach zone

This zone may take a variety of forms, and may not necessarily be a single direction of approach. Some examples include:

- A road approaching the front gate of a site or facility
- Pathway to the lobby of a corporate building
- Departures hall of an airport

1. **The approach zone**

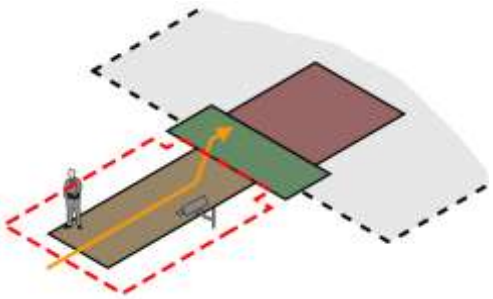


Figure 105 - Approach zone to a site

Key information

This zone should contain methods to detect potential security threats such as:

- CCTV Cameras
- Motion sensors
- Vehicle speed sensors
- Security staff

The approach zone will allow both Security staff and potential site users to prepare for Access control procedures. Signs and warnings may be placed in this zone to help potential site users behave as required within the Access control zone

11.5.1.2. The access control zone

This is where the authorisation of personnel or vehicles is checked against access permissions, and a decision made to grant or deny access. Examples of the access control zone include:

- Customs and immigration control at an airport
- Entry gate at a sports stadium
- Entry gate at an industrial site

Key information

This zone should contain:

- Queuing and movement control
- Security screening (additional methods of detection)
- ID inspection
- Physical barriers to progress

The placement and location of these features will depend on the type of site or organisation, but consideration should be given to:

- Threats and risks present e.g.
  - Level of security screening required
  - Spacing out of incoming traffic (foot or vehicle) to reduce casualties in event of catastrophic attack
- Hardness of physical barriers e.g.
  - Rope or chain
  - Barrier arm
  - Turnstile
  - Heavy vehicle barrier
- Volume of traffic (foot or vehicle)
  - Space required within the ACP
  - Turn around lane for access denial
  - Separation lanes for different site users

Events within the access control zone will determine whether a person or vehicle is permitted to proceed, and a well-designed access control zone will assist security staff to efficiently and safety grant or deny access

2. The access control zone

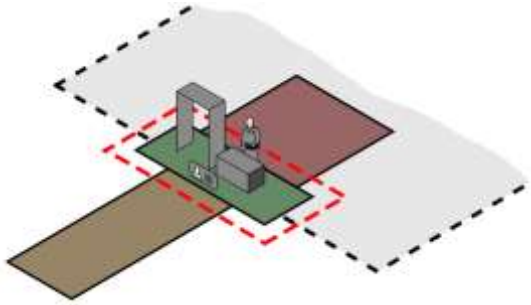


Figure 106 - The Access control zone

11.5.1.3. The response zone

This is the area in which Security staff and systems are planned to respond to breaches within the access control zone. If a security threat passes through the access control zone, the response zone is designed as a buffer to provide response time, and deny access to critical areas. Examples of a response zone include:

- Car parking areas placed between an ACP and the entry point of a building or facility
- Secondary perimeter lines inside a military camp

Key information

The response zone should contain:

- Final denial barriers
- Enough space to allow response time

The design of this zone may take different forms depending on the site, organisation and existing risks and threats, however the methods used may include:

- Automatic barrier activation on access routes
    - Hostile vehicles
    - Secondary gates
    - Doors locked down
- Alarm activations
    - Security staff response e.g.
        - Rapid deployment of security teams
        - Release of guard dogs
    - Law enforcement notified

Detailed calculations can be made by Security managers to determine the depth and capabilities of a response zone according to the risks and threats identified, however Security staff knowledge of the design process should be enough that how the response zone works is familiar and make sense.

3. The response zone

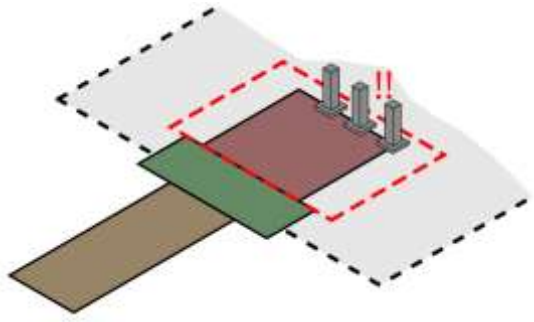
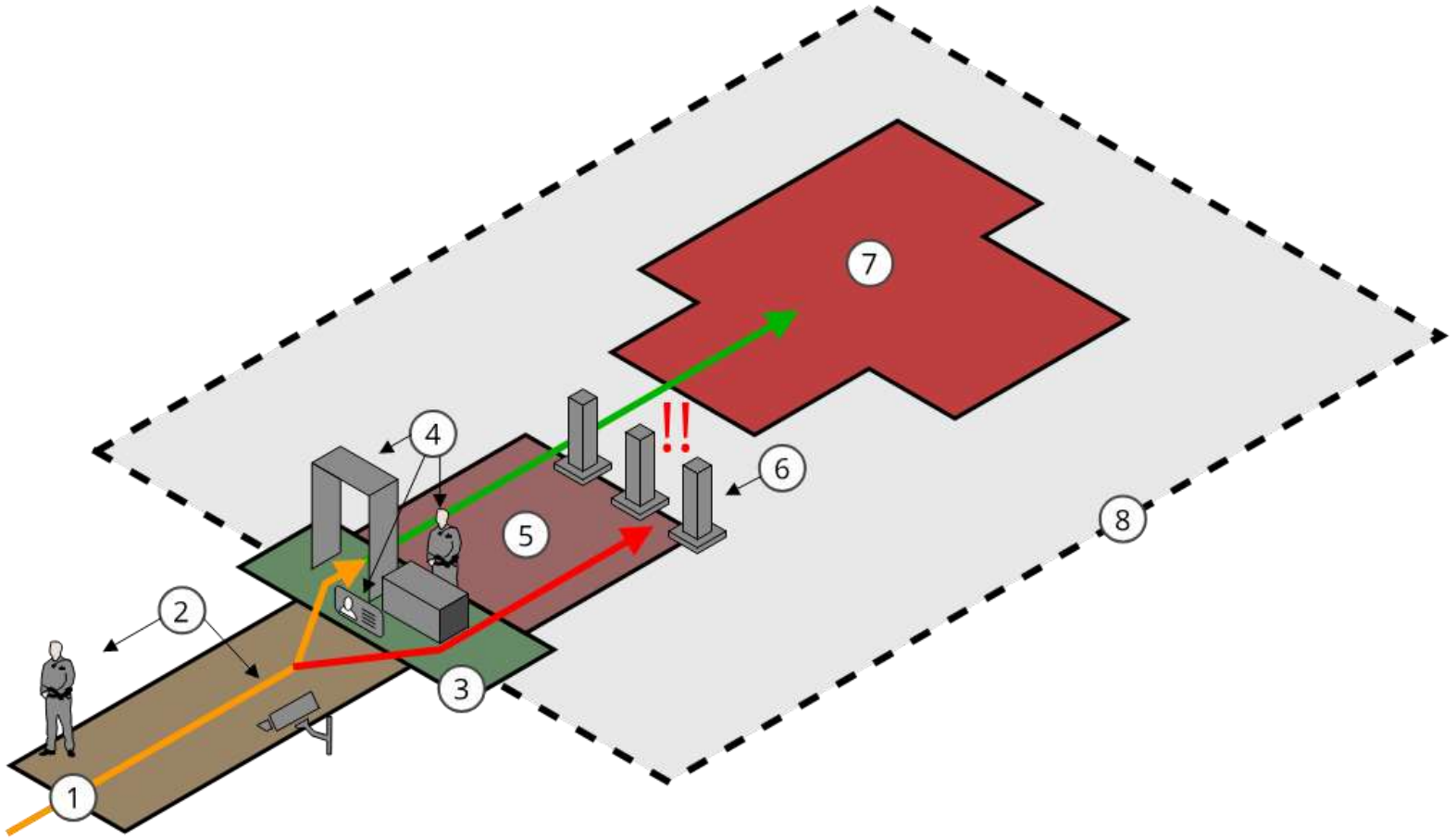


Figure 107 - The response zone

A complete diagram of an ACP is shown on the following page



	Incoming traffic	**1.** The approach zone **2.** Methods of detection **3.** The access control zone	**4.** Critical detection points **5.** The response zone **6.** Final denial barriers	**7.** Secured zone **8.** Perimeter forcing entry & exit through ACP
	Security cleared			
	Security breach			

11.6. Types of people and organisations requiring access

The types of people and organisations that may require access to a site or security controlled area will be different depending on each organisation. Security staff must become very familiar with the different categories of site user, and what locations, materials and resources they are permitted to access.

Key information

Most businesses, organisations and facilities may expect the following categories of user to require access at their site or building:

- Employees
- Customers
- Visitors
  - Planned e.g. appointments
  - Unplanned
  - VIP
- Contractors
- Maintenance
- Deliveries
  - Production materials
  - Retail Inventory
  - Company mail
  - Personal mail
  - Food

Each of these categories may arrive at the ACP with different vehicles, ID, access permission and entry routes.

11.6.1. Levels of access authorisation

The site access control policy will explain exactly who has access and where they are permitted to go. A site or building will normally be divided into access zones, and access permissions are issued to site users based on the operational and security requirements of the organisation.

Topic focus

A hospital example

Public zone – E.g. Carpark, Lobby, Cafeterias

- Users authorised
  - All
- Access controls used
  - CCTV monitoring
  - Security patrols

Reception zone – E.g. patient registration

- Users authorised
  - All
- Access controls used
  - CCTV monitoring
  - Reception staff
  - Security staff

Operations zone – E.g. Examination rooms, Wards, Offices etc.

- Users authorised
  - Employees who work in that
  - Security staff
  - Maintenance by appointment only
- Access controls used
  - RFID access card issued to Security staff and specific employees
  - Maintenance escort required

Security zone – E.g. Hospital control room, delivery loading area etc.

- Users authorised
  - Security staff
  - Delivery personnel by appointment
  - Employees who work in that location
- Access controls used
  - RFID + Passcode access issued to internally vetted staff
  - Delivery personnel escort required
  - Double door to enter secure zone

High security zone – E.g. Drug storage, medical waste storage, Data centres

- Users authorised
  - Doctors
  - I.T Technicians
  - Security staff
- Access controls used
  - Biometric reader
  - Secondary barriers e.g. Cage, locker, cabinet etc.
  - Unaccompanied access prohibited

This example shows how a Security manager and the organisational leadership may decide who can access what, and how that access will be controlled. Security staff will be aware of the levels of access granted to each category of site user and ensure that the access control policy is enforced correctly.

11.6.2. Handling visitors

The normal procedure for handling visitors will depend whether the visitor is planned, unplanned or a VIP, It will also depend on the type of site or organisation,

Key information

A standard method for Security staff working as Access controllers at the ACP is:

- Complete any pre-access control security screening (search, scan etc.)
- Identify if they have an appointment
    - If yes, confirm with the person who is expecting the visitor
    - If no, confirm what the visitor intends to do
- Confirm the identity by inspecting a valid ID e.g. Emirates ID, and record the ID details in the visitors' logbook
- Issue a visitors' ID badge and record the details of the badge issued
- Complete the remaining details in the visitor entry log
- Arrange for a security escort if required by access control policy

This method will work for most organisations, however the level of detail in security screening, badge issue, and escorting may vary depending on the risk and threat levels present.

11.6.3. Handling deliveries

When a delivery agent arrives at an ACP, Security staff will need to process the person and the items for delivery according to site SOPs. Normal procedures for the handling of deliveries will depend on each site or organisation.

Key information

A standard method for handling deliveries is:

- Carry out security screening of the delivery agent and the delivery package
- Confirm the delivery type e.g.
    - Parcel, mail, food, commercial goods
- Confirm the recipient and location within the building or site
- Verify that the delivery type is permitted to that area by the access control policy
- Verify the identity of the delivery agent by inspecting a valid ID e.g. Emirates ID & Company ID
- Record the delivery agent details, and consignment details in the visitor logbook
- Issue a visitor access badge, and record the badge details in the visitor logbook
- Call for the recipient to either;
    - Proceed to the ACP and receive the delivery or;
    - Prepare to receive the delivery at the required location on site
- Arrange for a security escort if required by site access control policy

11.6.4. Handling contractors and Maintenance teams

Contractors and maintenance teams may require access in order to carry out works within the site. Security staff should ensure that prior to allowing access, the personnel requesting access are processed correctly according to the site access control policy

Figure 108 - Site maintenance workers

Key information

A standard method for handling contractors and maintenance staff is:

- Carry out security screening of the personnel and any equipment
- Confirm the works required to be carried

out
- Inspect a Valid ID for each member of the working personnel e.g. Emirates ID & Company ID
- Record details in the visitor logbook
- Issue the appropriate access badges and record the badge details in the visitor logbook
- Inspect an authorised work order signed by the relevant person within the organisation
    - Verify the equipment permitted to be brought into the site for the works
    - Verify the safety requirements outlined in the work order
- Ensure only authorised equipment is in the possession of the work personnel
- Notify the work site area owner of the arrival of the contractor or maintenance team e.g. building manager, department coordinator etc.
- Arrange for a security escort if required by the site access control policy

11.7. Entry and exit control procedures

Security staff will be responsible for controlling entry and exit at secure sites, and the procedures required at specific sites may vary. Each site or location will have Standard Operating Procedures (SOPs), however the basic principles of control can be applied at any site

11.7.1. Standard operating procedures

SOPs will contain the information required to guide Security staff in performing duties at an ACP. The type of details contained within ACP Sops will include:

- Operating hours
- Categories of user permitted to use the ACP
- Security screening requirements
- Records and documents to be completed e.g.
    - Daily occurrence log
    - Visitor log
    - Incident report etc.
- Actions to take in response to risks, threats or other events e.g.
    - Theft
    - Dangerous items found
    - Receiving a delivery
    - Equipment failure
    - Evacuation procedure

Security staff will become very familiar with SOPs used at an ACP, and may offer help to Security supervisors or managers in improving existing SOPs

11.7.2. Processing entry to the site

At a site or facility requiring access control, Security staff will need to process each person or vehicle coming into the site in accordance with the access control policies.

Topic focus

Standard site entry procedure:

- Identify the category of person or vehicle approaching the ACP
- Confirm authorisation of this category to pass through this ACP
- Verify the ID of the person
- Complete the required security screening in accordance with site SOPs and the personnel/vehicle search techniques
- Assign a security escort if required
- Complete the ACP entry log including;
    - Name
    - ID details
    - Vehicle type if applicable
    - Vehicle registration if applicable
    - Location
    - Reason for accessing the site
    - Pass or badge issued
    - Security escort assigned
    - Time
- Open the barrier or gate allowing entry

Figure 109 - Access control point at a port

11.7.3. Processing exit from the site

The site exit process may include several different steps to the entry process, and

depending on the site may require another security screening (search) to be conducted.

Topic focus

Standard site exit procedure:

- Identify the category of person or vehicle wishing to leave the site
- Determine if this category requires further security screening on exit;
    - Search of vehicles
    - Search of belongings
    - Search of person
- Receive site pass, and record its return in the access log
- Record the time of exit
- Open the barrier or gate to allow exit

11.8. Escorting on site

Some sites may require that visitors, maintenance workers or other people that are not security cleared be physically escorted by a member of the Security staff while on site.

11.8.1. Escorting requirements

The need for security escorting will be determined by the site Security manager, and Organisational leadership, however Security staff must be aware of:

- Who needs to be escorted
- Which areas of the site require escort supervision
- The duties of a security escort

The purpose of security escorting visitors etc. is to ensure that vulnerable, sensitive or high risk areas are not left exposed to unattended visitors, and can effectively discourage:

- Theft or damage within the site
- Unauthorised access to controlled areas
- Photography or recording that is not permitted
- Completion of unsafe or unsecure maintenance works

If a site requires security escorting, Security managers must ensure that enough Security staff are available to support this task.

Key information

In some cases, security escorting may be provided by other employees within the site, relieving the Security staff of this added task. This would be clearly explained within site access control policies

11.8.2. Escorting procedures

If Security staff are tasked with providing escort to site visitors, there are several basic principles that should be followed:

Topic focus

Standard site escort procedure:

- Respond to an escort request, and attend the ACP
- Confirm receipt of responsibility for the visitor from the access control staff
- Confirm the location required to be escorted to, and the nature of the visit;
    - Person to meet
    - Work tasks to complete
    - Estimated timeframe
- Verify that the visitor is wearing the correct pass or badge
- Identify any tools, equipment or belongings that will be brought with the visitor
    - Re-check that all belongings remain with the visitor
    - Identify if any extra items or belongings have been added during the visit
- Communicate movement to and from the visit location with the control room
- Update the control room with any significant information;
    - Extended visit times
    - Changes to areas required to be visited
- Maintain vigilance throughout in order to prevent any dangerous, suspicious or criminal behaviour
- Return the visitor to the ACP
- Confirm hand over of responsibility for the visitor to the ACP staff

11.9. Access control point documentation

An ACP will keep several pieces of documentation as a record of the access control procedures being followed, and to highlight any incidents or equipment problems. Security staff must be capable of completing ACP documentation correctly and with accuracy.

11.9.1. Control point logs

The most commonly used method of recording who comes in and out of a site, area or facility is to keep an access log. This can then be used to verify who has been in a site, and how many visitors are still within a site at any particular time. An access log will contain standard information such as:

- Date, time
- ID details
- Name
- Who or where will be visited
- Reason for visit
- Site pass details

An example of this can be found at the end of this module

11.9.2. Incident reports

An incident report will be completed for any security incident such as:

- Breach of ACP
- Fight or assault
- Deliberate damage caused
- Prohibited items found

A standard form will be completed by Security staff, and then submitted by the ACP supervisor to the security control room.

An example of this can be found at the end of this module

11.9.3. Equipment maintenance and inspection logs

Security staff will need to conduct regular checks of the equipment and tools used within the ACP, and a log should be kept of these inspections for maintenance, servicing and warranty purposes. A common method of recording this type of information is to use a checklist for each piece of equipment to be inspected.

An example of this can be found at the end of this module

Example visitor log

#	Visitor Name	ID	Vehicle type	Registration	Place to visit	Reason for visit	Pass issued	Security Escort	Time in	Time out	Pass collected
1	Bilal Syed	987654321	Passenger car	65472	I.T department	Equipment sales	Visitor-Escorted	Mohammed Al Zaabi	10:25	11:45	✓
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											

Example incident report

Security incident report							
Incident ID	001	**Staff ID**	98765	**Name**	Mohammed Al Zaabi		
Date	2019-1-20	**Time**	10:05	**Map Zone**	5	**Map Grid**	A2
Type of incident		Prohibited items found			**Location**	ACP – Security screening point	

Incident description
During routine X-Ray inspection of baggage owned by site employee Mr Bilal Syed, a USB storage device was detected. This item is prohibited from being taken into the site in accordance with the Information Security policy.

Actions taken
The device was confiscated and stored in accordance with evidence handling procedures, and the device owner was informed that his department manager will be notified of the incident. The security control room was notified.

People involved		
Security staff	**Police & Emergency services**	**Public people**
Mr Mohammed Al Zaabi Mr Abdullah Al Maktoum	Nil	Employee: Bilal Syed Department manager: Robert Smith

Outcome of incident
The issue has been escalated to the site Security manager by the security control room supervisor for resolution with HR, employee manager and organisational leadership

Sent to supervisor	Hussein Al Otaiba – ACP Supervisor		
Filing location	ACP filing cabined	**Signature**	M. Zaabi

Example equipment inspection log

Daily Equipment Inspection Register			
Date	2019-1-23	**Equipment**	Access control barrier
Name	M. Zaabi	**Equipment No.**	SN01
ID No.	98765	**Equipment Location**	Access Control Point 1

Item to check	**Condition**		**Comments**
	✓	✘	
Remote controller is available and working	✓		
Manual controller is working	✓		
Barrier arm is straight and secure	✓		
Barrier turns on	✓		
Barrier arm lifts up	✓		
Barrier arm drops down	✓		
Check motor for signs of wear	✓		
Internal electrical wiring in good condition	✓		
External bolts and fixings tight and secure		✘	**2 bolts found to be slightly loose**

Module 11 Revision

Revision questions

1. List 3 examples of different types of people who may access a site

2. List 3 examples of different categories of vehicle that may access a site

3. Explain where a site access control policy will be kept

4. Explain who is involved in writing a site access control policy

5. List the 4 main roles within a Access Control Point

6. Give 3 examples of mechanical access control methods

7. Give 3 examples of electronic access control methods

8. Identify in the correct sequence the layout for an Access Control Point

(place a number next to each in the correct order)

The response zone

The approach zone

The access control zone

9. Summarise what the response zone is designed to achieve

10. List the 7 steps required to process a normal entry into a secure site:

1. Identify the category of person or vehicle approaching the ACP

2.

3.

4.

5.

6.

7.

11. Outline the details required to be recorded for entry into an access register

12. Give 3 examples of documentation used at an ACP

Module 3
Health and Safety

Module 12 Conflict management

Qualification Link

Units

- ADM03005NU17-Follow UAE workplace practice

Learning outcomes

1. Use effective interpersonal, social and culturally sensitive communication skills
2. Describe how use strategies to resolve conflict

Key definitions

Note: This module deals with personal conflict – NOT physical conflict situations which will be covered in a later module

Conflict – a state of disagreement between opposing ideas, people or interests

Resolution – the solving of a state of conflict with outcomes agreed by all parties

12.1. Conflict management policies

Security staff are in a position where they will certainly be exposed to conflict, and the skills and abilities required to solve these situations can be developed through awareness and practice.

Organisations will apply their own conflict management policies that will describe how internal conflict will be deal with, and these policies are normally produced by the HR department

12.1.1. Conflict management policy structure

Conflict management policies will contain the approved system for resolving a conflict in the workplace. The document will describe:

- Employee rights to a fair and equitable workplace
- Informal conflict resolution steps
- Formal resolution steps
- Timelines for conflict resolution

12.2. Dominant cultures in the UAE

A common cause of conflict globally is the coming together of diverse cultures with opposing views on religious, professional and social practise. Understanding the presence of different cultures will help Security staff to approach potentially difficult situations and avoid conflict where possible

12.2.1. Cultures frequently encountered

According to worldpopulationreview.com the UAE population as of 2019 is over 9.5 million people.

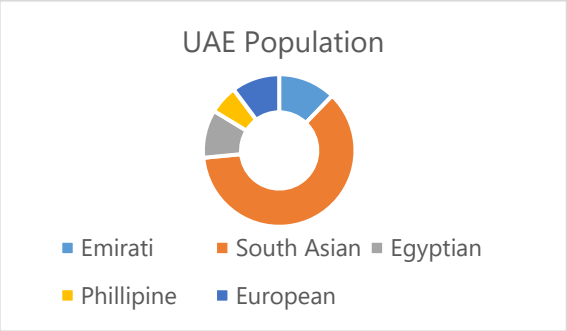


Figure 110 - Nationalities in UAE

As shown by this chart, there is wide range of nationalities present in the UAE and even more sub-cultures and religions.

The most common cultures encountered on a day to day basis are:

- Arab
- South Asian
  - Pakistani
  - Bangladeshi
  - Hindu
- European

Each of these cultures have different social and professional expectations. People who hold strong views based on their culture can easily become involved in personal conflicts with others in the workplace or team.

Security staff should always be aware of the differences between cultures within the team, working environment, and wider public in order

to remain respectful and avoid damaging relationships

12.2.2. Religious and social conventions

Recognising the requirements of others regarding religious practices and social etiquette will prevent unnecessary stress and offence, meaning another source of potential conflict can be avoided. Security staff should be aware of:

- Worship habits and locations
- Food and drink specific to a culture
- Clothing and accessories worn
- Days of religious significance

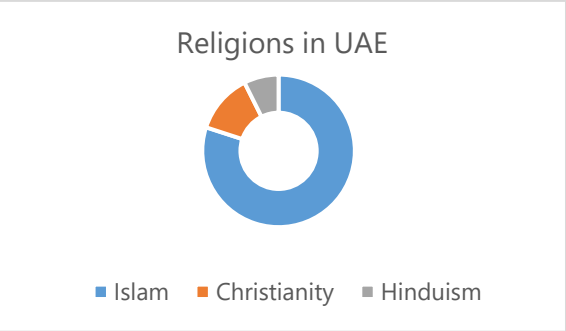


Figure 111 - Dominant religions in UAE

12.3. Recognising conflict situations

The ability to recognise situations that may cause conflict will increase the opportunity to prevent a conflict from ever happening. With practice and careful thought, Security staff will be able to identify potential for conflict, and take the necessary action to prevent it

12.3.1. Conflict environments

Conflict can happen in many environments, and for Security staff this is even more likely due to the role that is performed. The environments in which conflict is likely to occur can include:

- At the office
- On duty facing the public or other site users
- Within security posts e.g. control room or access control point

Maintaining awareness of where and how a conflict may occur will enable Security staff to reduce the likelihood, or respond appropriately ensuring the safety and security mission can continue without compromise

Figure 112 - Interpersonal conflict

12.3.2. Sources of conflict

Conflict can come from many sources within the environment of Security staff.

Key information

Conflicts may come from:

Internal work team

- Stress
- Verbal abuse
- Untidy workspace
- Tension between members
- Poor communication
- Lack of space or privacy

External sources

- Disrespectful employees outside the security team
- Deliberate aggression e.g.
  - Personal violence
  - Attempts to damage or destroy property
- Upset site visitors, contractors, delivery agents etc.

A key indicator of conflict is an emotional display, and these are often difficult to hide

from view. Any sign of a negative emotion from others may indicate the beginning of a personal conflict situation

12.3.3. Effective communication

One of the most common causes of conflict in the workplace is poor communication. Communication can be categorised into:

- **Verbal**
  - spoken communication
- **Non-verbal**
  - Written
  - Body language
    - Facial expression
    - Hand gestures
    - Posture etc.

It is important to note that non-verbal communication is interpreted just as clearly as verbal communication

Figure 113 - Nonverbal communication through facial expression

Effective communication relies on clear and complete sending and receiving of messages. Some methods that can improve the flow of communication include:

- Keeping duty occurrence books for situational awareness
- Publishing policy and procedure manuals for all to read
- Holding regular staff meetings to pass on information
- Distribute decisions made to everybody in the team
- Make sure team objectives and personal objectives are clear to everybody involved
- Spend twice as much time listening rather than talking

Figure 114 - Distributing information and decisions

12.4. Steps to conflict resolution

When a conflict has occurred between colleagues, customers or other people at the work site, Security staff must be equipped to resolve this situation in order to restore a healthy working environment

12.4.1. Methods of conflict resolution

There are many recognised methods of resolving personal conflicts, and each will have strengths and weaknesses. 5 well known approaches to resolving conflict are:

- **Collaboration method** – This strategy brings together the common interests of each person to work together toward a common goal. This can take time and requires a lot of trust between the people involved
- **Compromise method** – This strategy involves each person being flexible about the final outcome of the conflict. This could be achieved more quickly
- **Competition method** – This puts the people in conflict into competition to prove who has the correct standpoint in the conflict. There is the risk that the loser of this competitive strategy will still feel unsatisfied with the outcome
- **Accommodation strategy** – This involves 1 person admitting to the other that they were wrong, or agreeing to disagree and move on.
- **Avoidance strategy** – This is simply putting the conflict to one side to be dealt with at a later time, hoping that the issue will disappear on its own.

Some of these strategies will be used by Supervisors or Managers to deal with disagreement or conflict between Security staff,

other employees or customers and members of the public.

12.4.2. Steps to resolve a conflict

Security staff can use 4 basic steps to deal with a personal conflict between themselves and others, or between 2 other parties.

Key information

An easy way to remember the steps is to think **SLOW**.

Set the tone

Listen and acknowledge

Observe and organise

Work toward resolution

Figure 115 - Finding a solution to conflict

Topic focus

Using the SLOW conflict resolution steps

Skill 1 – **Set** the tone of the conversation

- View the situation as a problem to be solved together – not a battle to be won
- Use positive verbal and body language
- Be aware of and control the natural instincts to be aggressive

Skill 2 – **Listen** and acknowledge

- Listen to the other persons feelings, emotions and experiences
- One of the biggest barriers to conflict resolution is when people are unwilling to acknowledge each other's perspective on the situation

Skill 3 – **Observe** and organise the situation

- Try to view the conflict as a 3rd person to understand the whole story
- Ask questions to better understand the opposing point of view

Skill 4 – **Work** to find a solution

- Once the issues causing the conflict have been clearly observed and organised, an open mind is required to see a solution
- Try to find a solution that will satisfy each person
- Many solutions may be identified, and each person may then agree upon a final solution

12.4.3. Reviewing the conflict resolution process

It is important to review the outcome to any conflict in order to ensure the lasting effect of the solution. This is usually applicable to conflicts that have occurred within a familiar environment, as each person will remain in contact and the potential for further conflict still exists.

Security staff can take time to evaluate if the agreed solutions are still valid, and remain aware of any further developments that may result in new conflict beginning, or old conflict restarting.

Figure 116 - Listen and acknowledge

Module 12 Revision

Revision questions

1. Name the department responsible for developing conflict management policies

2. List the 4 topics covered within a standard conflict management policy

3. List the 3 largest cultures by population in the UAE

4. Give 4 examples of religious or cultural practices that may be different

5. List 2 sources of conflict in a workplace

6. Give 3 examples of causes for internal team conflict

7. Give 2 examples of causes for external conflicts

8. Name to 2 types of communication

9. Outline the meaning of SLOW conflict resolution

   S

   L

   O

   W

Module 3
Critical incident response

Module 13

Critical incident response

Qualification Link

Units

- SEC04004NU18-Respond to emergencies and security incidents

Learning outcomes

1. Outline response protocols
2. Conduct emergency evacuations
3. Carry out response to security incidents
4. Apply physical intervention techniques
5. Implement cordon and control of incident sites
6. Employ reporting and monitoring procedures for offending persons

Key definitions

Critical incident – an incident that may cause significant disruption to normal operations, or serious harm to people property or information

Physical intervention – the use of physical force to prevent harm and ensure the safety and security of people, property or information

Dynamic Risk Assessment – The process of evaluating threats to health, safety and security in real time as a situation changes

Cordon – A temporary perimeter established to control access and exit from an incident site

13.1. Overview of critical incidents

Security staff must be trained and prepared to respond quickly and efficiently to any critical incident taking place. Others within the site, building or organisation will look to Security staff for direction and decisive leadership during a critical incident situation.

Examples of a critical incident include:

- Natural disaster
- Acts of terrorism
- Robbery
- Assault
- Sabotage
- Severe accident

13.1.1. Impacts of a critical incident

What makes an incident critical is the impact it has on the business or organisation

Key information

Organisations may define what is critical to them in different ways, but often a scale or description is developed to measure what types of incident would be critical to the normal operations. Examples of how an organisation may be impacted by a critical incident include:

- Loss of production facilities
- Loss of personnel (through injury)
- Reputation damage
- Financial consequences
    - Cost of lost sales or production
    - Fines or penalties
    - Legal costs
    - Cost of repairing damages
- Reduced employee performance
    - Psychological damage
    - Distraction from work

These are just some of the impacts that a critical security incident can have, and it is clear that prevention is the ideal solution.

Security staff can reduce the impact of a critical incident through rapid and accurate response in order to:

- Reduce damage
- Isolate risks and threats
- Remove non-essential personnel from the area
- Coordinate emergency services response

13.2. Sector specific incidents

There are many examples of what type of incident could be defined as critical, however certain incidents are more likely to occur, and

have a critical impact within specific industry sectors or organisations

13.2.1. Educational Facilities

- Fire
- Serious illness / infection
- Armed attack
- Teacher strike
- I.T Breach or data loss

13.2.2. Government buildings

- Fire
- Mass protesting
    - Political or ideological
    - Disruptive to government services
- Terrorism
    - Explosive attack
    - Armed attack
    - Biological agent or chemical exposure
- I.T Breach or data loss

13.2.3. Critical Infrastructure

- Power failure
- Terrorism
- Sabotage
- Operating equipment or machinery damaged
    - Cooling systems
    - Fume extraction
    - Air circulation
- Fire
- Hazardous substance exposure

13.2.4. National borders and ports of entry

- Mass refugee migration
    - Asylum seekers
    - Border rushing
- Transport failure
    - Aeroplane groundings
    - Ships and vessels not seaworthy
- Severe weather
- Terrorism
- Outbreak of infection
    - Quarantine breach
    - Arrival of foreign disease
- Evacuation required
    - Control of personnel not cleared for immigration
    - Accounting for personnel

13.2.5. Sports clubs and stadiums

- Spectator violence
- Fire
- Terrorism
    - Bomb threats
    - Vehicle vs. Pedestrian
- Stampede
- Kidnapping or missing children

13.2.6. Hospitals

- Violent conduct requiring restraint
- Receiving hospital for mass casualty event (terrorism or natural disaster)
- Fire
- Outbreak of infection
- Missing patient (including children)
- Theft of controlled substances e.g. drugs/medicines
- Patient confidentiality breach

13.2.7. Banks

- Robbery
- Fire
- ATM Fraud
- I.T Breach or data loss

13.2.8. Hotels and Tourist sites

- Fire
- Violent conduct
- Terrorism
- Missing children

13.2.9. Museums and Cultural centres

- Fire
- Theft
- Terrorism
- Destruction of artefacts
- Failure of artefacts environment control e.g.
    - Humidity controller
    - Temperature controller
- Missing children
- Water leaks

13.2.10. Parks, beaches and public areas

- Violent conduct
- Severe weather
- Terrorism

13.2.11. Retail and commercial sites

- Theft
- Fire
- Terrorism
- Missing children

13.3. Incident response

Being able to identify a safety or security incident is only part of the job of Security staff, and the appropriate response must also be taken in order to maintain safety and security as effectively as possible

13.3.1. Principles of incident response

Incident response options will often vary depending on the site, organisation, industry and type of incidents, however the basic principles of response can be summarised and applied to each incident scenario.

Key information

When responding to any incident, Security staff should think about:

- Assessing risks to health and safety
- Reducing the risk of further damage
  - Physical
  - Reputational
  - Psychological
- Isolating the threats or hazards

13.3.2. Standard Operating Procedures

In order to make the decision making process for Security staff simpler, each site or organisation will a Standard Operating Procedures (SOPs) document prepared. The SOPs will guide the Security staff response and actions required to effectively respond to safety and security incidents. The SOPs will normally include information about:

- Actions to take in the event of each incident that has been planned for
- Who is responsible for each action
- Communication and reporting lines
- Triggers for escalating the control of incident sites to external agencies
- Returning to normal operations after an incident

13.3.3. Guides to specific incident response

The following section will offer a general guide that Security staff can follow in response to specific types of incident. These procedures will provide a reasonable level of detail for a general application, however at each site or place of duty, specific procedures will be in place that must be followed by Security staff.

13.3.3.1. Loss of power

If power is lost at the place of duty:

- Report immediately to the control room or site supervisor via radio or mobile phone
- Check that any access control/CCTV/intrusion detection systems are still working
- Ensure the security of any critical assets or property by either physical presence or remote monitoring
- If the area has become darkened:
  - Give instructions to other staff or employees discouraging non-essential movement
  - Deploy any available emergency lighting
- If personnel numbers permit, maintain control of the area, and deploy others to the electrical control panels to attempt re-setting of fuses
- Maintain vigilance and await the arrival of technicians
- Upon re-instatement of power, check and test any security systems for proper working status
- Report normal operations resumed at the place of duty to control room or site supervisor
- Prepare and submit an incident report

13.3.3.2. Trespassing

If the crime of trespassing is identified:

- Report immediately to the control room with:
  - Location
  - Quick description of offender
  - Direction of travel if moving
- Attempt to speak with the trespasser and:
  - Inform them that they are trespassing
  - Find out why they are in the prohibited area
  - Direct them to leave the prohibited area
  - Inform them that the police will be called if they fail to cooperate
  - Escort the trespasser from the area
- If the trespasser fails to comply with verbal directions:
  - Inform the control room of deliberate act of trespassing (police will be called)

- Maintain visual contact with the trespasser
- Update the control room regarding location and direction of movement
- Update the control room with more detailed description of the trespasser (A-H)
- Assess the risks present, and provide physical protection to other people, property or information as required

- Receive police officers at the site and hand over responsibility for detention or prosecution of the trespasser
- Record the incident details in the personal security notebook
- Prepare and submit an incident report

13.3.3.3. Violent behaviour

If any person is committing unarmed violence toward others:

- First, deal with the offender by:
  - Rapid physical intervention using defensive techniques (described in a later section)
  - Restrain the offender
- Report the incident to the control room, requesting additional Security staff to provide help (police will also be called)
- Separate and detain the violent offender
- Provide first aid to injured persons as required
- Begin the process of evidence gathering and witness statements
- Receive the police officers at the incident site and hand over responsibility for the offender
- Give the police any evidence and statements as required
- Record the incident details in the personal security notebook
- Prepare and submit an incident report
- Resume normal operations

Safety!

- When making the decision to use physical intervention techniques, always consider an escape plan should the offender be unable to be restrained

13.3.3.4. Suspicious behaviour

If suspicious behaviour by an individual or group is identified:

- Report immediately to the control room with:
  - Location
  - Description of person or persons
  - Description of suspicious activity

  (Further surveillance may be available through CCTV etc.)
- Maintain visual contact and continue to observe and report on the situation
- Assess any risks to the safety or security of other people, property or information
- Begin the process of recording observations in the personal security notebook
- Escalate the situation depending on updates to the observed behaviour by:
  - Reporting to the control room
  - Calling the police
  - Engaging with the suspicious person
  - Providing physical protection to people, property or information as required
- Complete recorded observations in the personal security notebook
- Prepare and submit an incident report

13.3.3.5. Hazardous substance exposure

If a hazardous substance is exposed in the place of duty:

- Assess the type of substance, and immediately establish a safety distance (several metres up to complete evacuation depending on substance)
- Report the incident to the control room
- Determine if the substance can be contained by Security staff in location

Safety!

- Wear any PPE that is required for this type of substance exposure
- Refer to the Material Safety Data Sheets for hazardous substances kept on site for the appropriate handling, treatment and disposal requirements

- Control access to the area and:

    - Dispose of the hazardous substance, or;
    - await the arrival of appropriately trained personnel to contain the substance
- Record incident details in the personal security notebook
- Prepare and submit an incident report

13.3.3.6. Intrusion alarms

If an intrusion alarm sounds:

- Verify the location of the alarm
- Silence the alarm
- Verify the intrusion through either:
    - CCTV surveillance of the intrusion alarm location
    - Dispatching Security staff to the location
- Upon confirmation of an intrusion:
    - Call the police
    - Attempt to locate the intruder(s)
    - Update all staff with locations or further details as available
    - Establish the security status of critical areas or assets within the intrusion vicinity
- If the intruder is found, refer to SOP for trespassing
- If the intruder is not found:
    - Search the site to find potential exit point
    - Search the area for;
        - Items left behind
        - Potential theft or removal of property
        - Damages
- Control access to the breach point
- Receive police offers and hand over control of the breach point for evidence collection and crime scene processing
- Prepare and submit an incident report

13.3.3.7. Fire

If a fire is detected:

- Raise the alarm
- Give clear and calm directions to other personnel to leave the area by the designated escape route, confirming that it is not blocked by the fire or other hazards
- Assess the potential for fighting the fire

Safety!

Before attempting to fight a fire, ensure that:

- Your escape route is not blocked
- All personnel are clear of the immediate area
- A general evacuation is already underway
- Activate a test burst from the extinguisher before approaching the fire

Assume that you will fail, and be prepared to escape!

- Search all rooms and toilets within the area of responsibility
- Ensure there is assistance given to people of determination
- Ensure all doors and windows are shut when leaving each area
- Carry out a roll call at the assembly point using attendance or access registers
- Prevent personnel from attempting to leave the assembly point
- Clear access for Civil Defence to approach and deploy at the site
- Record details of the incident in the personal security notebook
- Prepare and submit an incident report

13.3.3.8. Armed attack

If an armed attack is taking place:

- Report immediately to the control room with attacker details including:
    - Location
    - Number of attackers if more than 1
    - Direction of attack
- Delay the attackers progress by:
    - Locking down doors and access points
    - Locking internal doors
    - Barricading internal routes e.g. hallways and corridors

Safety!

- Direct other staff and visitors to internal safe points e.g. locked rooms, and instruct them to remain still and silent
- Maintain awareness of attackers' position and be prepared to move with other staff and visitors in order to maintain a 'zone' of delay

- Monitor and report the situation to control room in order to provide maximum situational awareness
- Provide first aid to any victims that are accessible without risking further casualties
- Await the arrival of armed response force e.g.
  - Police
  - Military
  - Armed private security
- Upon neutralisation of the threat, assist police and emergency services by:
  - Controlling access to the incident site
  - Preserving evidence
  - Providing witness statements
- Prepare and submit an incident report

13.3.3.9. Medical emergency

If a medical emergency is identified:

- Provide immediate first aid
- Send for help / report to the control room
- Continue to provide first aid until the arrival of emergency services
- Hand over the patient to paramedics with:
  - Circumstances of incident
  - Casualty condition
  - Treatment provided
- Record incident details in the personal security notebook
- Prepare and submit an incident report

13.3.3.10. Bomb threat

If a bomb threat is:

- **Received by phone**
  - Remain calm and keep the caller on the line as long as possible. Do not hang up, even if the caller does
  - Alert a colleague or other person that a bomb threat is being made
  - Listen carefully, be polite and show interest to the caller
  - Try to keep the caller talking to learn more details
  - If the caller number is displayed, make a note of the number
  - Complete the bomb threat checklist
  - Immediately call the police
- **Received by handwritten note**
  - Call the police
  - Handle the note as per evidence handling methods
- **Received by email**
  - Call the police
  - Do not delete the message

Note 1: The bomb threat checklist is available at the end of this section

13.3.3.11. Suspicious package or device

A suspicious package or device may be received by delivery, or left unattended. Signs of a suspicious device include:

- No return address
- Stains
- Strange smells
- Strange sounds
- Unexpected delivery
- Notes giving strange delivery instructions

If a suspicious package, object or vehicle is identified:

- Assess the potential for explosive damage (amount of explosive that could fit inside)
- Determine the appropriate safety distance, and begin to direct others to a safe distance
- Send a message to the control room via runner or landline telephone

Safety!

- Do not use a radio or mobile phone – radio signals may trigger detonation of a bomb
- Do not activate the fire alarm – an observer may be watching and trigger the bomb if an alarm is raised

- Control access through the establishment of a security cordon
- Record as much detail as possible about the object including:
  - Type of object e.g. backpack, briefcase, motorcycle etc.
  - Size
  - Location
  - Circumstances of discovery
- Await the arrival of police and hand over control of the incident site

- Continue to control access to the incident site until the all clear has been given by police
- Prepare and submit an incident report

Safety!

Minimum blast safety distances for objects:

Object	Shelter location	
	In building	Outside
Pipe bomb	25m	350m
Vest	50m	500m
Briefcase/bag	60m	500m
Motorcycle	80m	500m
Car	100m	500m
Small truck	200m	1000m
Water truck	270m	1500m
Semi-trailer	500m	2800m

- Distances have been calculated using maximum explosive capacity for an object of this size
- When sheltering inside of buildings, people must stay away from windows, doors and other openings.

Figure 117 - Suspicious bag left in carpark

13.3.3.12. Building evacuation

If a building evacuation is required:

- Collect critical security items:
  - Radios
  - Access logs
  - keys and access cards
- Direct others in the workplace to secure their workspace
- Direct others out of the building using the established evacuation routes
- Conduct a quick search of the area of responsibility for any personnel remaining
- Exit the building and proceed to the designated assembly area
- Hand over access logs to the building duty supervisor for accounting
- Ensure no personnel attempt to re-enter the building
- Control access to the building through an established security cordon
- Record incident details using the personal security notebook
- Prepare to hand over responsibility for the incident site to arriving police or emergency services
- Prepare and submit an incident report

13.3.3.13. Site evacuation

If a site evacuation is required, this will involve the closure of the security control room if it is housed within the site to be evacuated. Consideration should be given to this during site security planning, and an alternative control system identified. This may include:

- Maintaining a secondary control room on standby offsite for critical incidents requiring evacuation
- Establishing a temporary command and control post on the ground outside the site

If a site evacuation is ordered:

- Secure critical items to be taken during the evacuation
  - Access cards and keys
  - Access logs
  - Radios and communication devices
- Lock down the area of responsibility
  - Control room
  - Access Control Points
  - Critical security zones
- Move through the area of responsibility ensuring all personnel are following the evacuation order
- Conduct a final search of the area to verify no personnel remain on site
- Move to the external assembly area and hand over personnel accounting tools e.g. access logs
- Establish and maintain a security cordon around this site
- Control access to the site and do not allow any personnel to re-enter

- Await the arrival of police or emergency services
- Hand over control of the site to emergency services
- Record incident details in the personal security note book
- Prepare and submit an incident report

Key information

It is essential that Security staff are well trained and confident in the actions required by site SOPs in the event of a safety or security incident. Security supervisors and Managers will be responsible for the training and rehearsal of incident response for a site. Site specific training drills should:

- Be carried out at least every 3 months
- Involve all personnel who are expected to perform a role in the response
- Be evaluated for effectiveness after rehearsals
- Be recorded in a site incident training log

Topic focus

The most important considerations for every incident response procedure are always:

- Assessing safety and security risks
- Clear and accurate communication
- Acting with confidence
- Reassessing safety and security
- Limiting damage and containing threats

Example bomb threat checklist

Date		Time	
Time caller hung up		Phone number where call received	
Ask the caller:			
▪ Where is the bomb located			
▪ When will it go off			
▪ What does it look like			
▪ What kind of bomb is it			
▪ What will make it explode			
▪ Did you place the bomb	**YES**	**NO**	
▪ Why			
▪ What is your name			
Exact words of the threat:			

Information about the caller:		
Callers voice	**Background sounds**	**Threat language**
☐ Angry ☐ Calm ☐ Clearing throat ☐ Coughing ☐ Crackling voice ☐ Crying ☐ Deep ☐ Disguised ☐ Excited ☐ Female ☐ Laughing ☐ Lisp ☐ Loud ☐ Male ☐ Normal ☐ Rapid ☐ Slow ☐ Slurred ☐ Soft ☐ Stuttering	☐ Animal noises ☐ House noises ☐ Kitchen noises ☐ Street noises ☐ PA systems ☐ Conversation ☐ Music ☐ Motors ☐ Clear ☐ Static ☐ Office machinery ☐ Factory machinery	☐ Incoherent ☐ Reading a message ☐ Taped recording ☐ Irrational ☐ Profane ☐ Well-spoken
Other information		

13.4. Cordon and control of incident sites

A security cordon can be used to control an incident site, and provide greater situational awareness of what is happening both within and outside of the cordon.

Note 1: A security cordon is sometimes called a secure perimeter.

13.4.1. Incident cordon principles

Key information

The basic principles of establishing a security cordon are known as the 4 C's

- Confirm
- Clear
- Cordon
- Control

Depending on the incident site, an inner and outer cordon may be established to provide a system of zones within the incident site with different levels of access authorised for each. Examples of where this may be applied includes:

- Large fires where support crews require access to the site, but only firefighters move into the inner cordon
- Explosive device disposal sites where law enforcement and security staff operate within the site, but only the technicians operate within the inner cordon

13.4.2. Establishing a cordon

In order to establish a security cordon, the purpose for the cordon must first be determined. This will then result in the following questions being answered:

- What is access being restricted from?
- How much distance is required from that item or area?
- How many Staff are needed to effectively control access?
- Where is the incident site command post going to be located?
- Are physical barriers and markings going to be required?

When an incident has occurred that requires the establishment of a security cordon, this will be coordinated by the site security supervisor or manager, and Security staff must be prepared to receive instructions on where to move and occupy a position within the security cordon.

Topic focus

The principles of a security cordon are applied as follows:

Confirm the presence of a threat or risk requiring the evacuation of an area or incident site

- May be confirmed by visual inspection
- May be confirmed over the radio
- May be confirmed by other witnesses or observers

Clear the area

- Direct all personnel out of the area
- Check the immediate area to be occupied on the security cordon for any threats to health or safety

Cordon the incident site

- Place barriers or tape if required
- Maintain intersecting lines of visibility with other Security staff
- Conduct radio checks with the incident site command post
- Verify positions held on the cordon line and adopt new radio callsigns as appropriate

Control access through the cordon line

- Prevent unauthorised movement through the cordon line
- Log and record all personnel who enter or exit the incident site

An example diagram of a security cordon for an incident site is included at the end of this section

13.4.3. Maintaining a cordon

With the security cordon in place, Security staff must maintain the integrity of the cordon in order to effectively control the incident site.

Topic focus

Things to consider when maintaining a security cordon include:

Duty post rotation

- Increases vigilance and attention to detail
- Prevents boredom during long incidents

Passage of information

- Alert all Security staff if personnel are passing into or out of the security cordon
- Provide situational awareness to the control room
- Situation updates sent to the incident site commander

Sustainment of the cordon

- Refreshments for Security staff on duty
- Relief in place by incoming shift staff

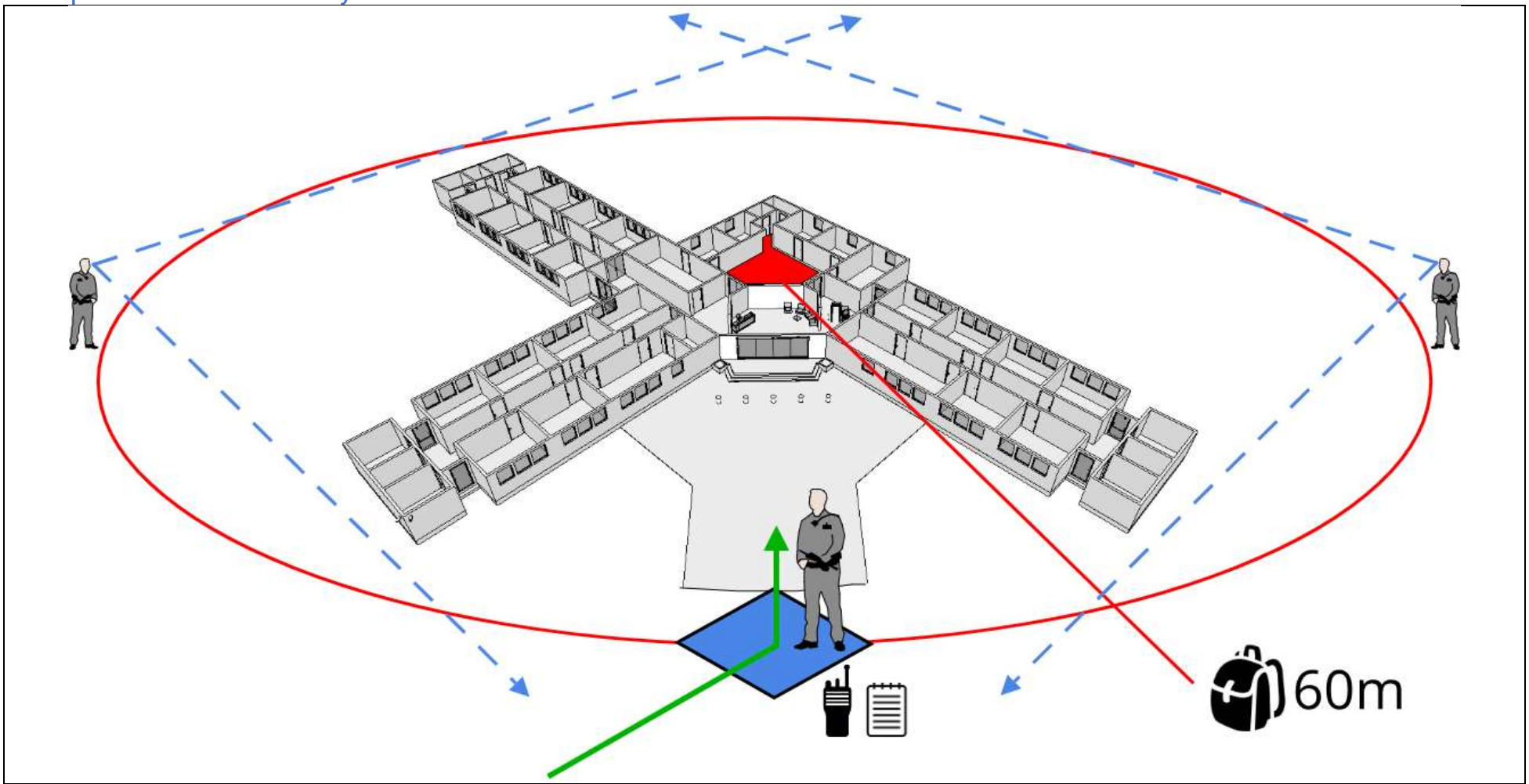
13.4.4. Collapsing a cordon

When an incident has been resolved, and the area has been deemed safe to re-enter, the security cordon may be collapsed. When the order is given by the incident site commander, Security staff who have been occupying positions on the cordon line will:

- Acknowledge the cordon collapse via radio
- Retrieve any barriers or tape that were used
- Move to the required duty location
- Report repositioning to the control room
- Await instructions to contribute to a post incident debriefing with the incident site commander
    - Security staff may be relieved by replacement personnel in order to attend debriefing
    - Incident notes and recorded observations should be brought to debriefing sessions
- Resume normal security operations

If an incident is significant enough that an evacuation and security cordon were conducted, incident reports will be prepared by site Security supervisors and Managers, however Security staff may be required to prepare and submit an incident report, and should be prepared to do so using written notes and observations.

Example incident site cordon layout



	Incident site command post
	Cordon line set at minimum safety distance for object / item / device / substance
	Entry control point for incoming emergency services
--	Intersecting lines of visibility for cordon Security staff

13.5. Monitoring and reporting ongoing situations

The most effective response to ongoing safety or security incidents will include accurate monitoring and reporting on the situation. Security staff must be skilled in providing these updates to the control room and other colleagues in order to provide the best possible situational awareness, without taking up too much time on the radio

13.5.1. Providing situation reports

When providing a situation report during an ongoing incident the following should be kept in mind:

- Keep radio communication brief and to the point
- Report only changes to the previous situation e.g.
    - Personnel locations
    - Suspect or offender locations
    - Behaviour or activities
    - Changes to the risk or threat levels
    - Any other significant updates

This will ensure that important changes are communicated, but the radio channels remain as free as possible for others to also utilise

13.6. Cooperation with emergency services

Security staff will often have close cooperation with emergency services such as police, firefighters or paramedics. It is important that Security staff are aware of the role that the emergency services will perform and how to best cooperate.

13.6.1. Preparing for the arrival of emergency services

During a safety or security incident where the emergency services have been requested to respond, Security staff will begin to prepare for their arrival. Factors to consider will depend on the type of incident and who is responding, however a basic outline for preparation includes:

Police

- Securing any evidence on site
- Preparing accurate incident notes
- Preparing recorded evidence e.g. CCTV footage, photos etc.
- Segregating witnesses, offenders and suspects
- Clearing routes and parking space for arriving police vehicles

Civil Defence

- Preparing maps or diagrams of the source of fire within a building
- Clearing routes to hydrants, breeching inlets and stairwells
- Maintaining public order at the site or building

Ambulance/Paramedics

- Recording casualty conditions including
    - Circumstances of medical incident
    - Medical history
    - Treatments given during first aid
- Clearing routes to the incident site

13.6.2. Handing responsibility to emergency services

When handing over responsibility for an incident to arriving emergency services, Security staff will need to:

- Provide as much detail as possible
- Record details of attending emergency staff including:
    - Names
    - ID
    - Contact numbers
    - Branch or office
- Obtain a receipt for any materials or evidence provided to police

Figure 118 - Empty handed self-defence

13.7. Self-defence and physical intervention

Security staff may find themselves in harm's way or in a situation where intervention is required in order to ensure the safety and security of others. It is vital that Security staff are able to apply self-defence and physical intervention methods safely and with confidence

13.7.1. Principles of self-defence

Physical intervention may only be used if the following four conditions are met:

1. There is an unprovoked attack
2. Injury or death is probable
3. A reasonable degree of force is used in response
4. A reasonable fear of injury or death is assessed

This interpretation of the law also allows for pre-emptive use of force in self-defence if the threat of attack is reasonably justified.

Key information

A key concept in the application of force for self-defence is known as the use of force continuum. It is a method for describing what amount of force is appropriate for the threat that is presented.

This scale of force is continually re-assessed by Security staff and the option chosen to match the level of threat presented.

Figure 119 - Empty handed wrist hold

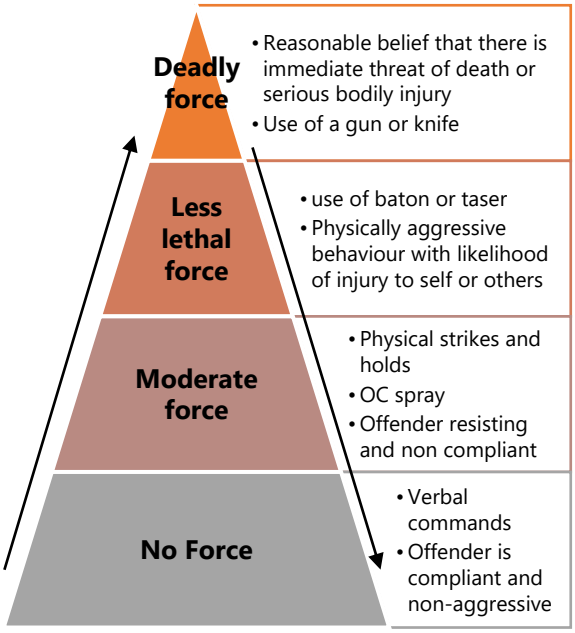


Figure 120 - Use of force continuum

13.7.2. Empty handed defensive techniques

The first level in escalating use of force is the application of empty handed defensive techniques. This includes techniques such as:

- Arm or wrist locks
  - Used to restrain and escort an offender
  - Used to control before applying handcuffs or restraints
- Defensive strikes to the nerve centres
  - Used to repel an aggressor
  - Attempt to disable the use of arms, legs and brain functions
- Kicks to the hip crease to disengage an attacker
  - Create distance between defence and attacker
  - Discourage further aggression
- Disarming techniques
  - Remove a knife or gun from the attacker
  - Neutralise the threat of deadly force

Topic focus

When the situation calls for the use of force, Security staff must be prepared to apply it correctly and with confidence. This will come through the repetition of realistic training and practice.

The main asset a defender has is time, as this allows the defender to make decisions and re-evaluate options. When confronted with an aggressor, Security staff should always attempt to maintain what is known as the reactionary gap. This gap will vary in size depending on the threat.

Reactionary Gap Distances	
Unarmed threat	2m
Impact weapons:	4m + Length of the weapon
▪ Pipe	
▪ Bat	
▪ Stick	
Edged weapons:	8m
▪ Knife	
▪ Sword	
▪ Axe	

Safety!

- Making the decision to attempt disarming of an attacker is very serious, and should be considered as a final resort
- The majority of disarming attempts result in the defender getting cut or shot

Figure 121 - Knife attacker

13.7.3. Using OC spray in self defence

The next level in escalation of force is the use of OC spray. This tool is highly effective at distracting aggressors and causing visual impairment

Key definitions

OC – Oleoresin Capsicum, is an inflammatory agent derived from organic chemical compounds found in various forms of potent pepper plants

Figure 122 - OC Spray device

Key information

OC Spray facts:

- Active ingredient is Capsaicin, the heat bearing and pain producing component of the spray
- OC Spray device also contains propellant gas and water to carry the active ingredient
- Is non-flammable, and can be used together with Electronic Control Devices e.g. Taser
- Is effective from 1 – 6 metres
- Does not physically stop:
  - Drug induced aggressors
  - Mental health aggressors
  - Highly motivated aggressors
- Affects 3 main areas:
  - Eyes
  - Skin
  - Respiratory system
- Will produce:
  - Involuntary eye closure
  - Extreme tears
  - Visual impairment
  - Coughing
  - Tightening of the chest

Secondary effects

The use of OC spray on an aggressor may result in possible psychological effects including:

- Fear
- Anxiety
- Panic
- Hyperventilation (Rapid breathing)

Exposure ratings

Exposure to OC spray is categorised by levels of contamination that include:

- **Level 1** – Direct into the eyes and face
- **Level 2** – Indirect contact with a person who has been exposed to level 1
- **Level 3** – Environmental exposure, mist in the atmosphere

Delivery systems

OC spray devices are configured to deliver the agent in different forms:

Liquid/Gel stream or;

Fog cone

Topic focus

Deploying OC spray in self-defence

For liquid/gel stream device:

- Spray sideways from ear to ear across the aggressor's eyes
- At 1.5m the spray diameter is 15cm
- If the aggressor is wearing glasses, spray just above the glasses on the forehead. The agent will then run into the aggressor's eyes

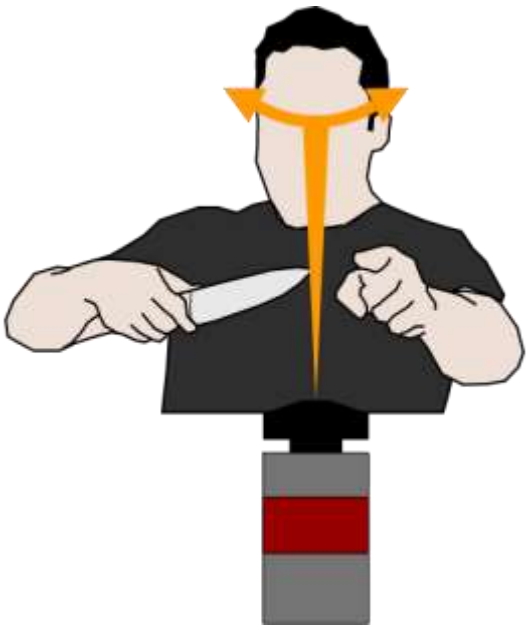


Figure 123 - Liquid stream spray pattern

For a fog cone device:

- Spray up and down the centre of the face
- Restricts the aggressors deep breathing
- At 1.5m the cone has a diameter of 30cm
- Be aware of wind direction
    - May blow agent back toward self
    - May blow across and contaminate non aggressors

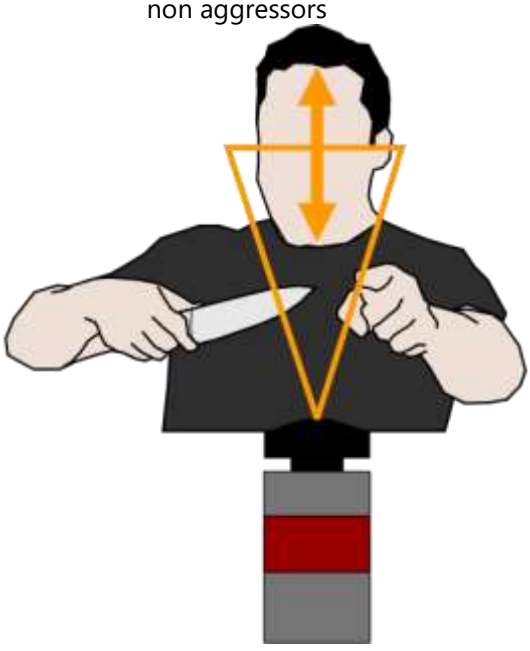


Figure 124 - Fog cone spray pattern

Treating OC spray contamination

To provide treatment to a subdued aggressor or others who have been exposed, use the following procedure:

- Expose skin and face to fresh air
- Flush eyes and face with large quantities of cool water
    - Hot water will open the skin pores and increase burning
- Wash skin with soap and water
- Remove contaminated clothing,

Figure 125 - Flushing OC spray from the eyes

13.7.4. Using a T-baton in self defence

Figure 126 - T-Baton

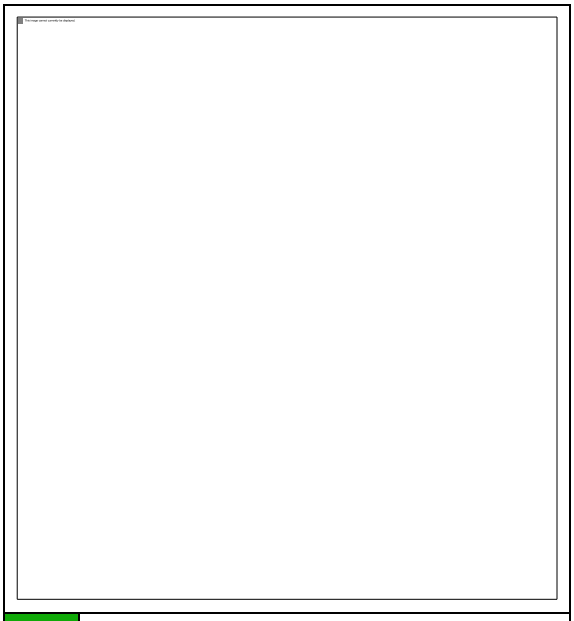
Key definitions

Strong side – The dominant side of the Security officers body e.g. Right hand and leg

The T-Baton is a self-defence tool designed to allow for strikes and blocks. The states of readiness for self-defence with a T-baton can be categorised as:

- Holstered baton
- Stand by positions
- Guard positions
- Defensive strike techniques
- Defensive block techniques

T-Baton strike zones



	Minimal level of damage, injury tends to be temporary rather than long lasting
	Moderate to serious level of damage, injury is normally more long lasting, but may also be temporary
	High level of damage, injury may be serious and long lasting, may include unconsciousness, shock or death

Topic focus

Self-defence methods with the T-baton

Holstered baton

- Fixed to the duty belt
- May be cross drawn or drawn from the strong side

Stand by position

- The baton is held in the strong hand, down and parallel to the strong leg in a ready stance
- The baton is protected by the strong leg from disarm
- The baton can be quickly raised into the guard position

Guard position

- The baton is held in the strong hand, over the strong shoulder, with the baton handle facing toward the aggressor
- From this position the baton can be brought forward for defensive strikes or

blocks

Defensive strikes

- The baton is brought down over the shoulder onto the selected target area
- The baton should be aimed so that the top portion of the baton makes contact with the target area
- Security staff should always direct defensive strikes to the appropriate body area depending on the threat presented
- Poorly aimed strikes will only provoke the aggressor
- Between strikes, the guard position should be used to maintain control and retain the baton from disarming
- The purpose of defensive strikes is to temporarily incapacitate the aggressor allowing safe withdrawal or restraint

Defensive blocks

- Overhead strikes by an aggressor can be blocked by moving the baton across the head in a defensive position and holding the end to catch the aggressor strike
- Low strikes by an aggressor e.g. kicks can be blocked by crossing the baton across the centre of the body and holding the end, then pushing down and away toward the aggressor strike
- Having blocked an aggressor strike, Security staff should re-establish the reactionary gap and adopt the guard position

13.7.5. Using handcuffs to restrain an offender

The use of handcuffs or other restraints may only be used by Security staff to secure an aggressor who has been caught red-handed in a criminal act. Security staff must be familiar with the techniques of applying handcuffs and restraints.

There are several variations of handcuff in use by different agencies in the UAE including:

- Handcuff
- Plastic cuff
- Textile restraint

Handcuffs are most commonly used by the police, however Plastic cuffs and textile restraints may be used by Private security staff.

Figure 127 - Types of handcuff and restraint

Safety!

Safety considerations for the use of restraints include:

Gaining control of the suspect prior to fitting restraints

- Use appropriate arm and wrist locks to gain control of an uncooperative aggressor

Proper tension of the restraint on the wrists

- The restraint should be tight enough to control the aggressor, but not completely restrict the flow of blood through the hands

Safe removal of restraints

  - The restraint should be removed using specialised cutters designed for that purpose

The process of applying restraints to an offender can be broken into 4 parts:

- Attitude
- Protection
- Communication
- Support

These 4 principles should be used to guide the process of restraining an aggressor or offender

Attitude

- Approach the aggressor from the side
- Be ready to react or withdraw
- A physical hand search of the aggressor will identify any risks of harm or escape e.g. a blade

Protection

- A second member of the Security team should provide a protective watch for the restraining staff.
- A 130-degree angle between restraining and protecting members should be maintained in order to allow good vision of the aggressor at all times

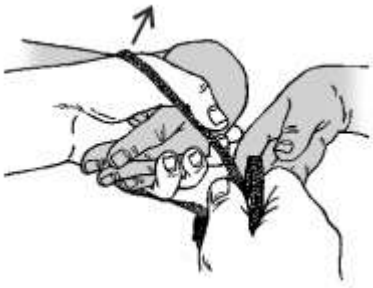
Communication

- Both restraining and protection personnel must maintain constant visual and verbal communication
- The restraining staff will give directions to the protecting staff to assist where required
- The restraining staff will also give direction to the aggressor being restrained

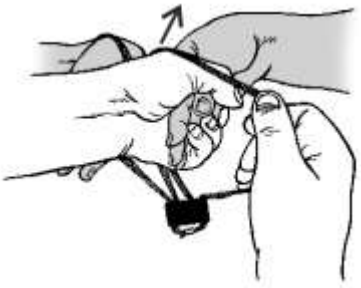
Support

There should always be two Security staff present in order to provide proper support in the event of aggression or non-compliance

Step 1: Restraint ready



Step 2: Capture 1 hand with the looped restraint



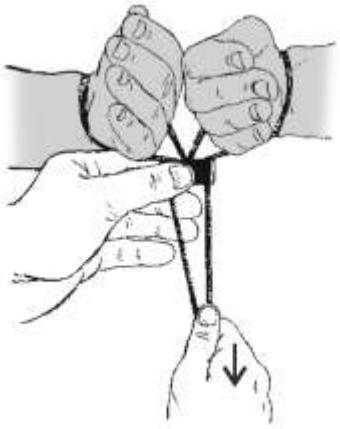
Step 3: Capture the second hand

Topic focus

Using textile restraints

Restraining the offender

- Position the offender using voice commands or physical holds
- Ensure the protection staff is in position
- Prepare the restraint as shown



Step 4: Tighten the restraints

- Check the restraints are tight enough, but not stopping blood flow through the hands
- Position the offender in a comfortable posture and begin processing the incident scene

Releasing the offender, use the purpose designed restraint cutter

Module 13 Revision

Revision questions

1. Define what is a critical incident

2. Outline 3 impacts that a critical incident might have on an organisation

3. List 3 specific examples of a critical incident at a national infrastructure site e.g. Nuclear energy plant or Oil Refinery

4. Outline the type of information that is found in SOPs

5. List the 3 principles of critical incident response

6. Identify 4 potential indicators of a suspicious package or device

7. List 3 items that should be secured and taken during a site evacuation

8. What should NOT be used if a suspicious package is identified?

a. Land line telephone
b. Radio & Mobile phone
c. Handwritten messages

9. What do the 4 C's of a security cordon mean?

C

C

C

C

10. What is the minimum blast safety distance for a backpack sized IED if sheltering in a building?

11. What are the 4 levels of the Use of Force continuum?

12. What four conditions must be met before

using force in self-defence?

13. What is the reactionary gap distance for an aggressor with a metal pipe?

14. What is the effective range of an OC Spray device?

15. Describe the method of deploying a liquid/gel stream OC spray against an aggressor

16. Outline the treatment given to a victim of OC spray exposure

17. When using a T-baton for defensive strikes, what zone is the head, neck and spine?

GREEN / YELLOW / RED

18. List the 4 principles of restraining an offender

19. Describe how textile restraints should be removed from an offenders wrists

Module 14
Cash in transit

Module 14

Cash in transit

Qualification Link

Units

- Nil

Learning outcomes

1. Identify the roles of a C-I-T team
2. Recognise the motivation of criminal behaviour
3. Identify the equipment and resources of a C-I-T operation
4. Outline the basic principles of C-I-T operations
5. Identify potential threat sources to C-I-T

Key definitions

CIT – Cash in Transit, the movement of cash or other valuable cargo between locations

CIT Crew – Security staff who have at least 1 year of experience in general security and are trained in CIT operations

CIT Crew leader – The member of the CIT crew who is in charge of the task

CIT Container – The box or case in which cash or valuables are transported

Cash centre – The bulk secure storage facility for collected cash and valuables

ATM – Automated Teller Machine, cash dispensing machine

BR – Bullion run, the daily trips taken by CIT crews to transport cash and valuables

Pavement – the area between the Armoured vehicle and the point of cash delivery or collection where the courier and escort move by foot

Attack – A direct assault by criminals on a CIT crew, vehicle or cash holding devices and personnel

Armoured vehicle – A vehicle that has been hardened to withstand fire, unauthorised intrusion and attack in accordance with PSBD regulations

Central control room – An operations monitoring room that is manned at all times

Cash in Transit (CIT) is a specialised security service providing a method for the transport of cash and valuables for banks, retailers and other businesses or individuals who require collection or delivery of their cash and valuables. This essential task enables a safe and controlled method of ensuring that the economic and financial patterns of operation are maintained.

Key information

CIT has 3 principles for operating

- Stay safe
- Do not discuss the work
- Stay in the vehicle

Figure 128 - Example CIT companies operating in the UAE

14.1. Roles and responsibilities of a C-I-T team

Within an organisation providing a CIT service, there are 2 main categories of Staff:

- Administration
- Operational

14.1.1. Administration

Administration roles are used to maintain organisation of the CIT operation, and tasks include:

- Licensing and compliance
- Business administration
- Accounting
- Asset management e.g. vehicles, cash centres, staff etc.

14.1.2. Operations

Operation roles refer to the tasks and activities conducted by the CIT crews including:

- **Driver –** responsible for navigation, driving and parking the armoured vehicle, and securing the vehicle
- **Courier** – Carries the CIT container while walking
- **Escort** – walks with and protects the courier

Figure 129 - CIT crew prepare to unload a CIT container

Topic focus

The CIT crew responsibilities include:

- Communication with cash owners for pick up or delivery
- Communication with central control room during BR trips
- Protection of cash and valuables
- Wearing and maintaining protective equipment
- Controlling or repelling potential criminals with empty hands and defensive tools
- Preparing and submitting security and BR reports and documentation
- Undertake secure loading and unloading of cash in a variety of environments
- Maintain vigilance against the threat of;
    - Hold ups
    - Hostage situations
    - Worker stress
    - Health and safety hazards

Figure 130 - Armed men robbing a CIT crew

14.2. Criminal behaviour and motivation

In order to effectively protect against theft and criminal activity, the behaviour and motivation should be understood by CIT crews.

14.2.1. Threats to C-I-T

Threats can be as serious as a planned and organised robbery, or a health and safety incident to the CIT crew while carrying cash. Awareness of potential threats will enable CIT crews to resist and succeed in their CIT tasks.

Key information

Potential sources of threat to a CIT operation

- Planned attack and robbery
    - Individual criminal
    - Group of criminals
    - Organised crime ring
- Opportunity theft
- Vehicle accident
- Accidental injury to CIT crews e.g. slips, falls, crushing or pinching of limbs

14.2.2. Crime in the UAE

There are cases of major robbery recorded in the UAE. These cases serve to remind CIT crews that robbery and crime is a real threat to the security of cash and valuables, and that these items present temptation to all kinds of people. Examples of major incidents in the UAE include:

- ATM Robbery in Sharjah
- Police officer shot and killed
- Armed robbery of a cash centre for AED 10m

- Robbery of wafi city jewellery
- Internal theft by CIT crew
- Multiple attacks on banks, ATMs and CIT vehicles
- Suicide bomber partnered with bank robber
- Robbery of millions of Riyals at Dubai Cargo Village
- CIT crews attacked with an axe
- CIT crews attacked with OC spray

Attacks on CIT crews can occur at any time and place, while mobile in the Armoured vehicle or while on the pavement.

14.3. Planning for C-I-T Operations

When preparing to carry out a CIT task, crews must be aware of the requirements of the task including legal obligations, equipment and tools required, and logistic considerations

14.3.1. Laws and regulations

Key information

The PSBD is responsible for the licensing and inspection of CIT companies and its employees.

The conduct of CIT operations in the UAE is governed by Chapter 3 of Ministerial Decision no. 557 of 2008 on Private Security. This chapter clearly provides laws regarding:

- The requirement for approved licences of companies and staff to work in CIT including:
  - Security guard licenses
  - Cash centre licenses
  - Armoured vehicle licenses
- Approval of CIT business buildings and facilities
- Sufficient staff to run the operations including:
  - CIT Manager
  - CIT Vehicle servicing employee
  - Internal security inspector
  - CIT Vehicle fleet leader
  - Communications technician
  - CIT crew
  - Site security for CIT business building and facilities
- Using approved cash transport boxes
- Procedures for CIT crews while in the vehicle
- Breaks and rest procedures for CIT crews
- Procedures for vehicle breakdown
- Cash centre requirements including
  - Cash centre manager
  - Shift manager
  - Internal security inspector
  - Cash crew
  - Communication technician
  - Security for the building

14.3.2. Equipment and resources

Topic focus

Equipment and items required for CIT

Documentation

- Staff ID from the company
- Bank ID
- Police information card
- Delivery/Collection documents

Personal Equipment

- Personal radio
- Alternate communications e.g. mobile phone
- Helmet with visor
- Body armour
  - Stab proof vest
  - Arm guard
  - Elbow guard
  - Gloves
- T-Baton
- OC Spray

Task equipment

- Armoured vehicle
- CIT container
- Coin bags
- Hand held receipt scanner/printer
- Tamper devices e.g.

Figure 131 - Example CIT equipment

14.3.3. Coordination with stakeholders

Clear coordination procedures are vital for the success of a CIT operation. This includes communication with:

- Central control room
- CIT leader
- CIT driver when Courier and Escort are on pavement
- Cash owners e.g.
    - Bank staff
    - Shop managers
- Cash centre

A well-defined plan for communication with these personnel will provide the best situational awareness to CIT crews and the central control room

14.4. Basic principles of C-I-T

The CIT operation can be divided into 2 parts:

- Vehicle mounted
- Dismounted (on foot)

Some basic security principles applied to these 2 parts of the operation will provide the best opportunity for a successful CIT task.

Figure 132 - GPS tracked armored vehicle route

14.4.1. Vehicle operations

Before starting CIT tasks

When preparing to use the Armoured vehicle to complete a CIT task, the crew should inspect:

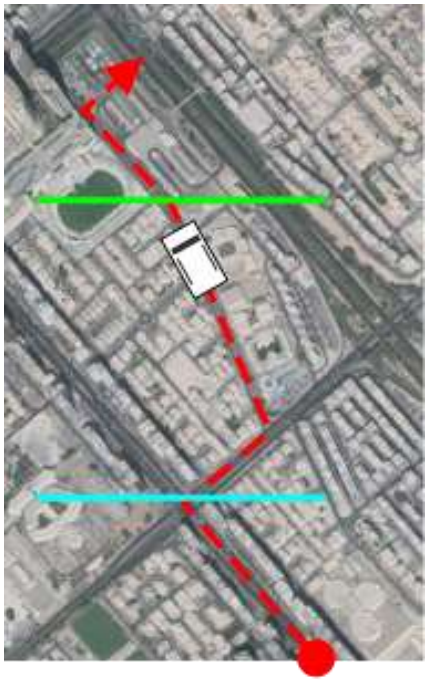
- Fitted security equipment is fully working
    - 360 cameras
    - Access locks
    - GPS system
    - Alarm system
    - Vault and compartments
    - Dummy bags and CIT containers
    - Radio communications
- Vehicle condition is good
    - No leaks from engine compartment or excessive exhaust
    - Signals and lights working
    - Escape hatch operational
    - Tyre pressures set
    - Refuelled and filler cap locked
    - Windows clean
    - Interior clean and organised
- Cargo is secured in place
- Weight and Cash value limits are not exceeded

While on the road

When mounted in the armoured vehicle, crews should:

- Report progress through scheduled communications checks
    - Use established reference codes, not actual place or location names for security purposes

- Update the central control room if expected arrival times change for any reason e.g. traffic, route diversion etc.
- Maintain 360 awareness of the vehicle surroundings
    - Driver and crew responsible
    - While moving, or stationary
- Report and record any suspicious or unusual observations
- Increase vigilance while stopped at traffic signals or intersections



Report line blue

Report line green

Figure 133 - Example of communication reporting lines in progress

Arriving at the collection or delivery site

When approaching the intended dismount point, crews should:

- Visually scan the area for potential risks and threats
- Report arrival to the central control room
- If no immediate threats are identified, the Escort can get out and;
    - Walk around the car looking for risks or threats
    - Perform a secondary visual scan of the area looking for threats
    - Present a professional and vigilant image
    - Signal the Courier to get out with the CIT container

Safety!

- Parking and unloading from the armoured vehicle presents a high risk for accident or safety incidents
- Drivers should ensure enough room to safely unload
- Escort and courier should remain aware of other traffic using the area

Key information

The size of a CIT crew may vary but a common example is:

- 1 x Driver
- 1 x Courier
- 3 x Escort

The size of the crew will determine the available escorting formations while dismounted

5 Person Crew:

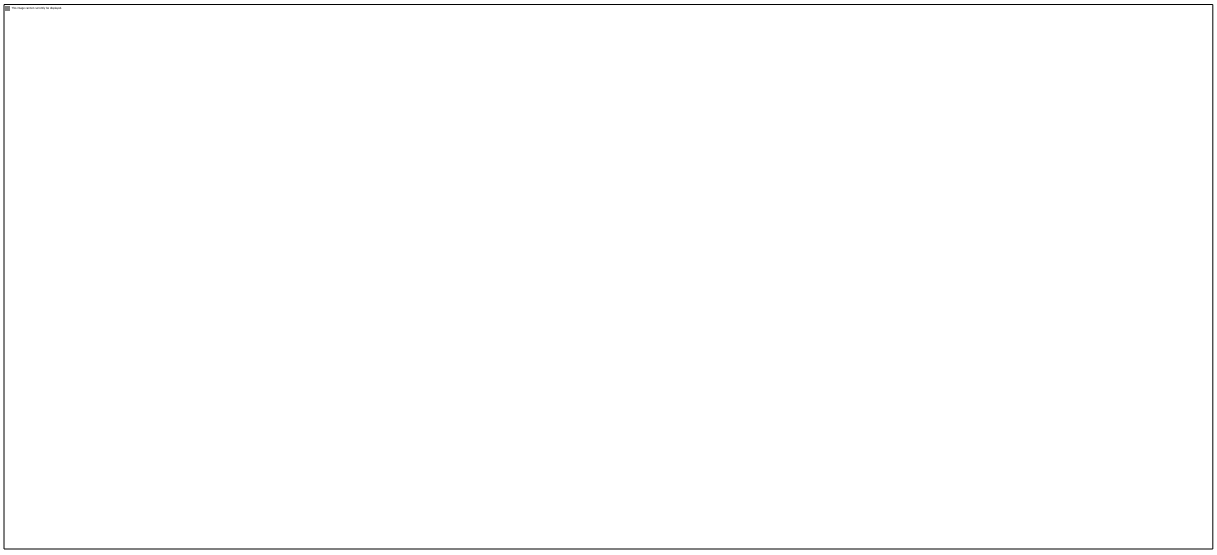
- 4 x Escort
- 1 x Courier

- Square/Diamond walking formation

4 Person Crew:

- 3 x Escort
- 1 x Courier

- Triangle walking formation



3 Person Crew:

- 2 x Escort
- 1 x Courier

- Single file walking formation

Figure 134 - Example CIT crew formations

14.4.2. Dismounted operations

Having arrived at the collection or delivery point, the CIT crew will dismount the armoured vehicle and move across the pavement and into the cash transfer area e.g. Shop, ATM, bank.

Topic focus

While moving from the armoured vehicle to the transfer area

- Ensure all protective equipment is worn correctly
- The T-Baton is carried in the standby position
- Move quickly to the transfer area
    - Adopt an appropriate walking formation for the route
    - Provide a buffer zone of protection for the courier
    - Do not stop for any reason except in an emergency
    - Be vigilant to threats, including diversions
    - Be prepared to take an alternate route or return to the armoured vehicle

When at the transfer area

- The escort team will
    - Radio check with the driver confirming safe arrival
    - Complete collection or delivery of cash
    - Secure CIT containers and receipt documents
    - Provide continuous surveillance and protection

- The driver will
    - Remain inside the vehicle
    - Not move the vehicle
    - Continue to observe and report on potential security risks

When returning to the vehicle from the transfer area

- The escort team will
    - Radio to the driver when ready to return to the vehicle
    - Adopt an appropriate walking formation for the route
    - Provide a protective buffer zone for the courier
    - Conduct a visual scan of the area surrounding the vehicle
    - Open the vehicle and load the CIT container

The entire CIT crew will now enter the vehicle and secure it. The CIT container will be secured in the vault.

The CIT crew will communicate with the central control room, informing of transfer completion and drive on to either the Cash centre or another transfer task.

Safety!

- Crews should take care for passing traffic or other roadside hazards when loading the CIT container

Key information

CIT crews should unload only 1 CIT container per trip to the transfer area. The CIT company will have a 'Pavement Limit' which is the amount of cash that can be taken outside the vehicle at a time. This amount is usually set by an insurance company.

Module 14 Revision

Revision questions

1. Name which chapter of Ministerial Decision no. 557 of 2008 deals with CIT Regulations

2. Name the 3 main roles within an operational CIT crew

3. List 5 pieces of personal equipment used during a CIT operation

4. Outline the 3 principles of CIT operations

5. List 3 sources of threat to a CIT operation

6. Which government organisation is responsible for licensing and inspection of CIT companies and staff?

7. Give 3 examples of who CIT crews should maintain communications with during a CIT operation

8. List 5 security features fitted to an armoured vehicle

9. List 5 checks to perform on an armoured vehicle before departing on a CIT task

10. When dismounted, the CIT Escorts should carry the T-baton in the standby position

TRUE / FALSE

11. When arriving at the cash transfer area, the CIT escort will radio the driver to confirm arrival

TRUE / FALSE

Module 3
Bank security

Module 15

Bank security

Qualification Link

Units

- Nil

Learning outcomes

1. Identify bank security principles
2. Apply visual screening methods within a banking premises
3. Outline bank security zones
4. Outline roles and responsibilities of security at a bank
5. Identify the relationships between bank security and C-I-T crews

Key definitions

OPZ – Outer public zone

IPZ – Inner public zone

PZ – Private zone

ATM – Automated teller machine

HVAC – Heating, ventilation and air conditioning

PIN – Personal Identification Number

Tiger kidnap – Kidnapping a persons loved ones or relatives to force them to carry out a crime to ensure safety of the kidnapped person

15.1. Introduction to bank security

Throughout history, banks have been seen as attractive targets for criminals due to the potential for a high reward for their crimes. The presence of large quantities of cash and other valuables is a temptation for thieves. In addition to this, modern banking technologies mean that electronic funds are also vulnerable to exploitation. Security staff must be aware of the potential threats faced by banks.

Banks are located in a variety of locations throughout the UAE, and vary from small customer service centers through to large branches with cash vaults and teller counters.

Features of a bank that impact the security considerations include:

- Open to public
- Cash and electronic funds transactions
- Located in various and complex environments e.g.
    - Street front
    - Inside malls
    - At airports

Figure 135 - ADCB bank outer public zone

15.2. Banking security zones

In order to make sense of the approach to security at a bank, a system of zones have been used to define who is permitted to access different parts of the bank, and the security measures that go with each. This is a similar concept to the use of access control zones for a site or building as described in the access control module.

Key information

Typical bank security zones are:

- **OPZ** – the outer public zone
- **IPZ** – the inner public zone
- **PZ** – the private zone

Security staff may be granted access to all 3 zones, or may have limited access to certain areas within the private zone. Security staff must be aware of the areas they are permitted to access in accordance with the specific bank policy

15.2.1. Outer public zone

The outer public zone is used to describe physical space that is outside the structure of the bank. Features of the outer public zone include:

- Accessible by any member of the public
- May be monitored by the bank security control room, including coverage of:
    - Road
    - Parking areas
    - Footpaths
    - ATMs
- May be patrolled by bank Security staff

The outer public zone is the first layer of protection for vital assets within a bank, and physical security measures available to deter or deny a criminal from accessing the inner public zone include:

- Hostile vehicle mitigation bollards
- CCTV monitoring
- Security lighting
- Landscape design
- Presence of Security staff
- Rules of entry sign posted to increase CCTV monitoring effectiveness e.g.
    - No motorcycle helmets to be worn
    - No sunglasses worn

Figure 136 - Green symbolizing outer public zone - OPZ

15.2.2. Inner public zone

The next layer of protection for vital assets held in the bank is called the IPZ – inner public zone. This zone is the area that is accessed by the banks customers and staff. The IPZ will include:

- Lobby
- Customer service reception
- Cash teller counter
- Queues
- Staff offices/cubicles
- Internal ATM installations

Physical security measures available to detect, deter and deny a criminal the opportunity to carry out a crime include:

- Security staff
- Teller counter barriers
- Clear lines of sight into the IPZ from outside
    - Reduces ability to commit crime unnoticed from outside
    - Increases public awareness of what is happening inside the bank
- Greeting staff (Security or bank staff)
    - Visual screening of persons entering the bank
    - Able to interpret non-verbal communications on intent
- CCTV
- Silent alarms
- Exit control

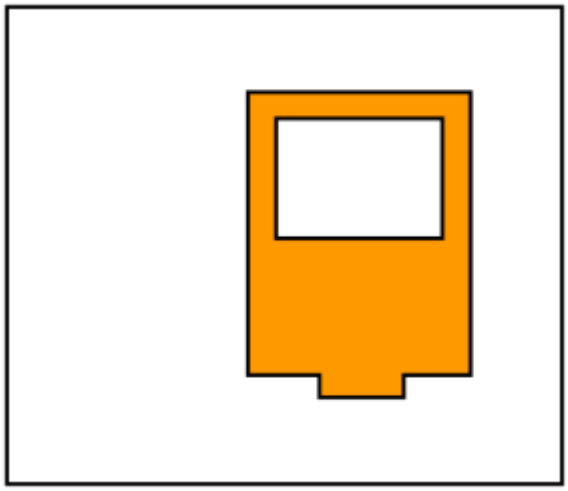


Figure 137 - Orange symbolizing inner public zone - IPZ

15.2.3. Private zone

The third layer of protection within a bank is the PZ – private zone. This security controlled zone will contain the most vital assets within a bank and is critical to the successful operations of a bank. The IPZ will include:

- Cash drawers behind the teller counter
- Vaults and Safes
- Cash cage
- Management offices
- Security control room

- May be full sized security control room or;
- May be small installation for remote monitoring from a central operations centre
- Networked CCTV equipment
- Integrated security and building management systems e.g.
  - Security alarms
  - Access and exit controls
  - Fire panels
  - HVAC monitoring

Physical security measures used to deny and delay a criminal attempt to commit robbery or other crimes include:

- Security staff
- Trained bank staff
  - Security policies and procedures
  - Threat response training
- Access control e.g.
  - Key card, PIN entry, Keys, Biometric access, Dual key entry
- Bullet resistant screens (teller counter)
- High security vault
- Security cash boxes with;
  - Dye packs for identification of stolen cash
  - GPS trackers
- Bait cash
  - Pre-recorded serial numbers for tracing of stolen cash

Key information

The transition between Inner Public Zone and Private Zone will always have a form of access control to prevent unauthorised personnel from entering

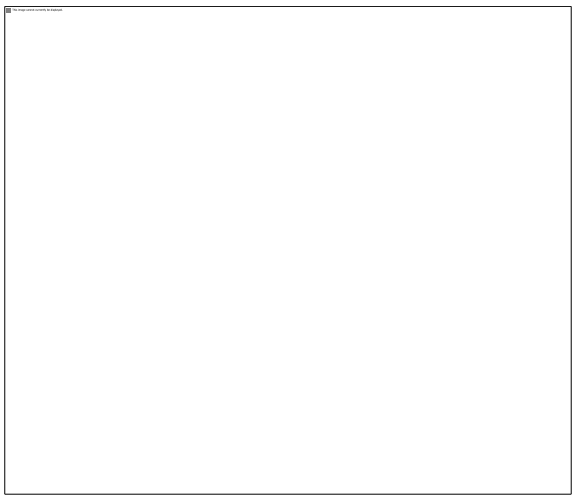


Figure 138 - Red symbolizing private zone - PZ

The 3 zones of bank security

	Outer public zone - OPZ
	Inner public zone - IPZ
	Private zone - PZ

15.3. Roles and responsibilities of bank security staff

Security staff working at a bank will maintain the basic principles of security, with some additional considerations specific to banking security.

Key information

Professional and vigilant Security staff will deter criminals from targeting the bank

15.3.1. Primary duties

Topic focus

The primary duties of Security staff at a bank include:

- Protection of property, people and information
- Detection and prevention of criminal activity through;
  - Screening of all persons entering within the OPZ and IPZ
  - Liaising with CCTV operators
- Detection and reporting of suspicious behaviour e.g.
  - Possible hostile surveillance
  - Targeting of bank customers
  - ATM fraud and tampering
- Response to safety and security incidents including;
  - Fire (lock down and evacuation)
  - Security systems failure
  - Medical emergencies
  - Aggressive and abusive customers
  - Attempts at robbery
- Securing the site of a crime scene
- Handling witnesses and evidence
- Cooperation with Police, Civil Defence
- Cooperation with CIT crews

Screening customers

Security staff can make assessments about customer intentions through:

- Visual search of each person e.g.
  - Clothing worn appropriate to situation
  - Bags or cases
  - Unusual shapes under clothing
  - Walking in an unusual way to conceal items
- Reading of a person's body language
  - Sweating
  - Hyper alert
  - Fidgeting and nervous
  - Fixed vision on a target area within the bank
- Welcoming and engaging in conversation
  - Get a feel for customer intention
  - Potential to identify trouble before it begins

15.3.2. Secondary duties

Security staff working at a bank will have the opportunity to contribute to safety and security through carrying out secondary duties within the bank. These include:

- Providing customer service
  - Ability to screen and profile people entering the bank
  - Get to know regular customers and identify changes in behaviour
- Direct movements within the bank e.g.
  - Flow of customers to banking offices/cubicles/teller counter

Key information

Bank security staff should cooperate with arriving CIT crews to ensure that:

- Secured parking is available
- Pre-screen the approach to bank
- Inspect all 3 zones for potential threats
- CIT crews are inspected for:
  - Valid IDs
  - Correct documentation

15.4. Bank crimes

The banking industry is exposed to unique types of crime and Security staff must be aware of the threats present in this industry in order to detect and respond appropriately.

15.4.1. Deliberate targeting of banks

The deliberate planning and targeting of a bank to commit crime can take many forms, and threats may include:

- Armed robbery
  - With a weapon
  - With the threat of a weapon
  - With a note passed to teller
- Small theft
  - Pickpocketing
  - Personal belongings e.g. hand bag
- Bomb threat
- ATM crimes
  - Card copying
  - PIN theft
  - False CIT crews/maintenance
  - Customer robbery
- Hostage taking
- Tiger kidnap
  - Crimes committed by an unwilling person who's loved ones are held by criminals
- Cheque fraud and theft
- Identify fraud and theft
- Fraudulent SMS posing as official bank communications e.g.
  - Requesting reply with customer details
  - Account information and PINs

Figure 139 - ATM Card copying device fitted over card slot

15.4.2. Crimes of opportunity

The bank may also offer opportunities for unplanned crimes, and Security staff should work to reduce the opportunity and attractiveness to commit these type of crimes including:

- Customers counting large sums of cash
  - Potential criminal may follow the customer to rob them
- ID documents left on counter or waiting areas
  - Potential identity theft or fraud
- Dropped or lost cheques/cash
  - Potential theft
- Cash left in the dispensing slot of an ATM
  - Potential theft

Security staff working inside a bank will quickly learn to identify examples that provide for unplanned criminal activities and can proactively work to reduce these chances

15.4.3. Insider threat

The threat of crime from insiders has possibly the greatest potential for loss for the bank. Staff who abuse their position and access privilege could carry out large scale theft and fraud. These types of crime have been documented in the UAE, and some examples include:

- Transferring funds from long unused customer accounts into personal accounts
- Assisting physical robberies with insider information and access
- Collection and release of personal customer information
  - This has been used to gain access to customer accounts and transfer funds illegally

Key information

Security staff can contribute to neutralising the insider threat by being fully aware of bank policy and procedure in order to:

- Identify and report bank staff not complying with security policies
- Identify unusual bank staff procedures
- Identify unlikely relationships between bank staff and potential criminals posing as customers

Module 15 Revision

Revision questions

1. List the 3 zones of bank security

2. Give 3 examples of what infrastructure is contained within the OPZ e.g. Roads.

3. Outline 5 examples of security measures to deter and deny criminals in the OPZ

4. Outline 3 examples of security measures to detect and deny criminals in the IPZ

5. Outline 3 examples of security measures to deny and delay criminals in the PZ

6. List 3 methods of security screening bank customers

7. Describe the steps that bank Security staff should take when cooperating with CIT Crews

8. Give 1 example of how Security staff can contribute to reducing insider threats at a bank

9. List 5 primary duties of bank Security staff

10. List 5 examples of bank crimes

Module 16
Hospital security

Module 16
Hospital security

Qualification Link

Units
- Nil

Learning outcomes
1. Identify Hospital security considerations
2. List threats and hazards to hospital security
3. Identify hospital security zones
4. Identify Hospital security incident colour codes
5. Outline infection control principles
6. Identify critical incident response procedures

Key definitions

Infection control – steps taken to reduce the chance of spreading infectious diseases

Caregiver – any personnel responsible for providing services to patients and their families

Access zone – designated areas within a hospital requiring authorisation and access credentials

16.1. Introduction to hospital security

Security staff assigned to protect people, property and information at hospitals and health clinics must acknowledge the complex environment and challenges that such a place presents.

The nature of healthcare means that a variety of stresses and emotions are present every day, and will contribute to the ability of Security staff to effectively perform their duties.

Specific roles and responsibilities may vary depending on the size, facilities and services that a hospital provides, however a typical hospital Security team may perform:

- Patient/ Customer service
- Access control
- Traffic control
- Internal and External patrols
- Emergency response
- Physical intervention & public safety
- Surveillance and investigation
- VIP escort and protection

16.2. Hospital specific threats and hazards

In order to effectively provide protection and safety, Security staff should be aware of threats and hazards that may impact the operational capabilities of the hospital.

16.2.1. Threats to hospital security

Security threats that hospitals may face vary in consequence, likelihood and risk, however the following threats would present a significant disruption to healthcare provision or hospital liability:

- Fire of any size
- Breach of information security & patient confidentiality
- Theft of medicinal supplies or equipment
- Abduction of children or babies
- Sabotage of life support equipment
- Contamination of food or water supplies

The mitigation of these threats will rely on a balanced combination of strong security policies and procedures, monitoring and control systems, and vigilance on behalf of the Security staff.

Figure 140 - Secure drug and medicine storage

Specific response procedures for security threats are described in a later section of this module

16.2.2. Hazards at a hospital

The hospital contains a variety of health and safety hazards unique to the healthcare industry, and Security staff must be aware in order to maintain safety and accurately report on potential risks on the site.

Different locations within the hospital will present different hazards, however each location should be inspected, and a risk assessment published by the health and safety management. Security staff can access these risk assessments and ensure that they are fully aware of the hazards as identified.

Key information

An overview of potential hazards

- Physical hazards
  - Slips and falls (most common in hospitals)
  - Traffic accidents in loading/unloading areas
  - Compressed or flammable gasses and liquids
  - X-Ray exposure
  - Electrical wiring and outlets
  - Patient or visitor violence
    - Mental illness
    - Substance abuse
    - Stress and worry
- Biological hazards
  - Used needles, surgical equipment
  - Blood and saliva
  - Infectious diseases
  - Deceased persons
  - Medical waste e.g.
    - Bandages
    - Soiled bedding
  - Allergies
    - Powder lined Latex gloves
    - Pollen from flowers
- Chemical hazards
  - Mercury spills from damaged medical devices
    - Portable blood pressure readers
    - Thermometers
  - Cleaning materials
- Psychological hazards
  - Stress
  - Fatigue
  - Burnouts
  - Death of patients

Security staff must be prepared to guard against non-clinical potential hazards, and the precautions to take will be specified by the hospitals policies and procedures, however for general guidance, refer to the health and safety module of this book.

Safety!

- Particular care must be taken by all members of staff to handle sharp items including needles with extreme care, and dispose of used needles in the designated containers

Safety!

Mercury is a metallic liquid element, and exposure can result in serious health risks. If Security staff identify any mercury spillage from a damaged medical device, the following containment steps should be followed:

- Evacuate everyone from the room, shut the door and turn off any ventilation system.
- Put on a face mask, remove any jewellery or lose items, and put on latex gloves
- Identify the type of surface the mercury was spilled on. Any absorbent surface needs to be disposed of
- Locate all the beads of spilled mercury, and use a piece of cardboard to push them together
- Use an eyedropper to suck up the mercury and dispense it into an airtight plastic container
- Place the plastic container in an airtight Zip lock bag, seal and label the bag
- Hand over to management for proper disposal

Note: In some healthcare facilities, such response is conducted by a team of experts that is dedicated to deal with hazardous spills.

Container	Contents
 **Sharps**	▪ Needles ▪ Broken glass ▪ Blades ▪ Razors ▪ Wires ▪ Other sharps
 **Biohazard**	▪ Blood ▪ Infectious waste ▪ Contaminated PPE ▪ Intravenous tubes
 **Chemotherapy trace**	Items in contact or containing chemotherapy ▪ Empty vials ▪ Empty intravenous tubes ▪ PPE ▪ Wipes ▪ Packaging
 **Pharmaceuticals**	▪ Pills ▪ Injectable medicine ▪ Antibiotics
 **Hazardous to environment**	▪ Hazardous medication ▪ Bulk chemotherapy ▪ Infectious disease exposed material

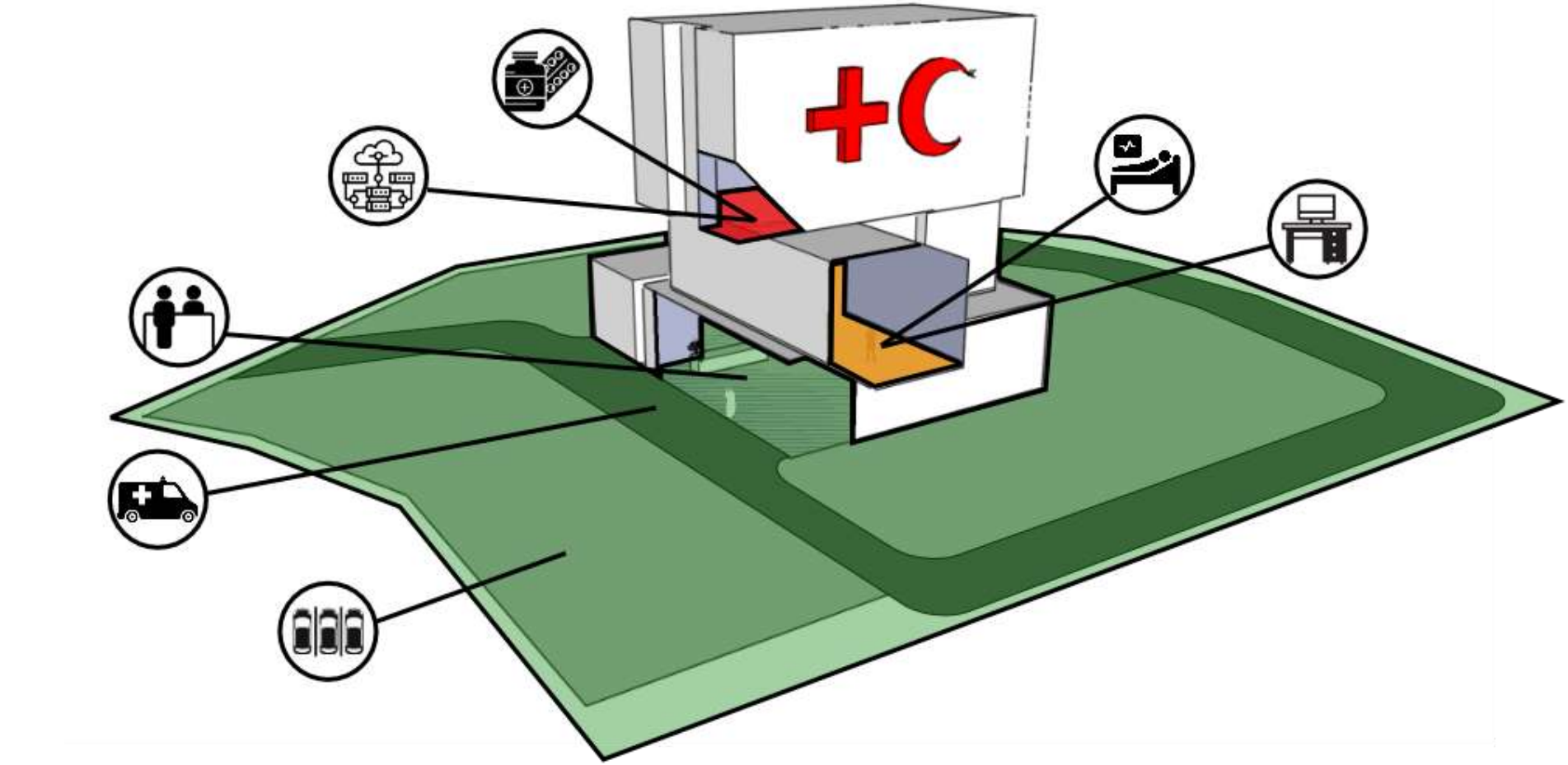
Table 19 - Hazardous waste disposal

Figure 141 - Spilled beads of mercury from a thermometer

16.3. Access control at hospitals

Access control at a hospital will follow the basic principles of physical security, however the zones and levels of access may be arranged according to the individual hospitals needs and requirements including:

- Staff and specialisations
- Building size and layout
- Site access points e.g.
    - Pedestrian
    - Vehicle
    - Ambulance
    - VIP
- Equipment and facilities
- Substances and materials stored in the hospital
- Assets Value and distribution



Public zone

Staff zone

High security zone

Figure 142 - Hospital security zones

16.3.1. Levels of access control

Key information

Public zone

Areas including:

- Drop off and pick up
- Parking
- Lobby and registration
- Cafeterias
- Patient wards

Users permitted:

- Patients
- Visitors
- All staff
- Deliveries

Staff zone

Areas including:

- Administrative offices
- Surgery/treatment wards
- Staff Break areas
- Clinical laboratories and Stations

Users permitted:

- Security staff
- Authorised staff (as per job requirement)
- Patients receiving treatment
- Pre-cleared and escorted contractors or maintenance

High security zone

Areas including:

- Main data centre – I.T Server Room
- Telecommunication Room (TR)
- Medical waste disposalLoading bays
    - Delivery and removal of medical equipment
- VIP wards
- Drug and medicine storage
- Security Control Centre

Users permitted:

- Security staff
- Authorised staff (as per job requirement)
- Pre-cleared and escorted contractors or maintenance

16.3.2. Entry control mechanisms

Apply entry/access controls to the different zones of security access can be achieved through the methods described in the Access control module, however typical control mechanisms found in hospitals include but not limited to:

- Security staff physical control of drop off and pick up zones
- Security staff physical control of Ambulance arrival zones
- Visitor registration and ID badge issue between public and staff zones
- Specific zone enabled RFID key card between different staff zones
- PIN code/Biometric access to high security facilities

Figure 143 - RFID Access card

16.4. Incident response

Security staff must be prepared to respond to a wide variety of incidents that can occur within a hospital operating environment. Training and site familiarity, along with strong knowledge of hospital SOPs will ensure that Security staff are able to respond quickly and safely, enabling the hospital to continue to provide care with minimal interruption.

16.4.1. Hospital Security Control Centre

The Security team will operate from a central security control centre (SCC), where the following roles and functions will be monitored:

- Parking and traffic areas
- Public gathering areas
- Security sensitive locations
- Elevators
- Security staff on duty
- Incident reporting and resolution
- Crowd control
- Entry and exit control
- Investigation

- Hospital incident management system (HIMS)

Security staff can expect to be in constant communication with the SCC while on duty.

Key information

The primary focus of security staff must always be the safety and protection of people, property and information, but this aim should be aligned with keeping the hospital operational in order to continue providing critical healthcare services to society

16.4.2. Standard incident codes

Common incidents have been planned for within hospitals, and a set of standard incident response plans developed for quick reference and communication to all personnel within the hospital. These plans are known by hospital staff as well as Security staff.

Key information

Standard hospital incident codes

Code	Event
Amber	Missing infant or child
Black	Bomb threat or suspect object
Blue	Unresponsive adult medical emergency
Brown	Hazardous material spill
Gold	Utility / I.T failure
Green	Internal disaster
Grey	Severe weather
Orange	External disaster
Pink	Unresponsive child or infant medical emergency
Red	Fire or smoke
Silver	Weapon or hostage situation
White	Violent person
Yellow	Missing adult

Hospitals will have developed SOPs specific for each site for responding to these incidents, however Security staff can refer to the incident response plan/module for general guidance on responding to these incident types

16.4.3. Common hospital incidents

Certain events and incidents occur more often at hospitals due to the nature of a high stress healthcare environment. Some examples of frequent incidents include:

- Code white – Violent person
- Code blue – Adult medical emergency
- Stroke alert – Patient showing signs of suffering a stroke

Incident response

Code white – Security staff will be directly responsible for resolving violent and abusive behaviour toward others within the hospital. This behaviour can occur frequently due to the stressful situations that family of loved ones, or mentally unwell persons can find themselves in. Hospital staff, other visitors and Security staff may find themselves subjected to violent behaviour.

Topic focus

Steps in response to code white:

- Control room will coordinate calling police if required
- Proceed to the reported incident location
- If violence is still ongoing;
    - Intervene using physical restraint methods
- If violence has stopped but the offender is still present;

- Separate the victim and offender
- Engage the offender in conversation and request their cooperation
- Provide first aid to the victim if required
- Request the offender remain in Security custody until the matter is resolved

- Secure any evidence, document and record the incident, and take witness/victim/offender statements

Code blue – Security staff will be required to act in a facilitation role in order to allow the rapid movement of emergency medical response teams, and controlling any family or bystanders

Topic focus

Steps in response to code blue:

- Proceed to incident location
- Provide first aid/CPR until relieved by emergency response team (ERT)
- Control the incident site (crowd control) allowing space for the ERT to perform duty of care
- Clear access through the hospital for ERT to move the casualty to the appropriate treatment area

Ensure only authorised personnel cross access control zones during transfer of the casualty

Stroke alert – stroke symptoms can be identify through FAST method

F - Face: Ask the person to smile. Does one side of the face droop?

A - Arms: Ask the person to raise both arms. Does one arm drift downwards?

S – Speech: Ask the person to repeat a simple phrase. Is their speech slurred or strange?

T- Time: If these symptoms are present, quickly report the stroke alert to nursing staff

If such symptoms appear in a person, an emergency stroke alert must be reported immediately to nursing team to ensure speedy response to such condition is achieved to save persons from severe health damage or death situation.

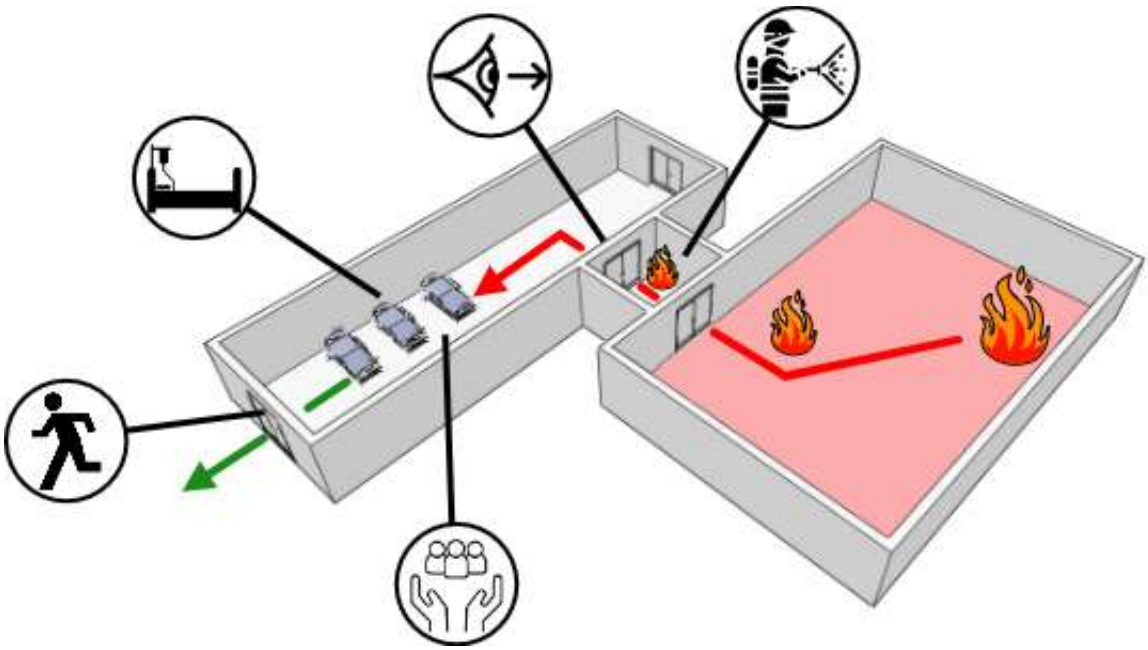
16.4.4. Critical hospital security incidents

Critical incidents that can occur in a hospital will have a major impact on the ability of the hospital to provide care for patients. Examples of critical incidents include:

- Code red - Fire
- Code green – Internal disaster - outbreak of disease or infection
- Code orange - external emergency
  - Natural disasters
  - Power outages
  - Mass casualty terrorism event

Incident response

Code red – fire is a very serious event within a hospital as it will threaten the ability to provide care for the ill and injured (patients), and can spread quickly. Security staff must be prepared to assist hospital staff in evacuating the affected area/relocating to adjacent safe zone,



Stage 1 – evacuate the immediate area, maintain caregiving capabilities

Stage 2 – monitor the situation and be prepared to evacuate further

Figure 144 - Example of relocation/evacuation stages during fire in hospital

Topic focus

Steps in response to code red:

- **R.A.C.E**: An **acronym** that hospital personnel use to remember their duties in case of fire.

If you are involved in a fire, remember **R.A.C.E.** to help you respond safely and correctly:
R = RESCUE: anyone in immediate danger from the fire, if it does not endanger your life
A = ALARM: sound the alarm by calling "2600" (on-campus locations only) and activating a pull station alarm box
C = CONFINE the fire by closing all doors and windows
E = EXTINGUISH the fire with a fire extinguisher, or **EVACUATE** the area if the fire is too large for a fire extinguisher.

- **P.A.S.S**: An **acronym** that hospital personnel use to remember their duties for discharging a fire extinguisher.

To use fire extinguishers correctly, remember the **P.A.S.S.** acronym:
P = PULL the pin on the fire extinguisher
A = AIM the extinguisher nozzle at the base of the fire
S = SQUEEZE or press the handle
S = SWEEP from side to side until the fire appears to be out

- Fight the fire if it is safe to do so
- Assist hospital staff to evacuate the area of all patients and staff through:
    - Advance clearance of evacuation routes
    - Guidance and direction to hospital staff
- Ensure the area is completely evacuated and shut all fire doors and curtains to isolate the fire
- Monitor and report on fire condition be prepared to evacuate to the next safe location

Note: It is not preferable to completely evacuate the building as critical life support facilities may not be able to be transported outside the hospital

Code orange – external emergencies may place a heavy burden on hospitals to provide treatment and are often made a central collection point for large amounts of casualties. In the event of a code orange, Security staff will be expected to provide direction and control within the hospital site, in liaison with civil defence, police and maybe even military personnel.

Topic focus

Steps in response to code orange:

- Occupy access control points at hospital entries
- Screen entering personnel for access permission based on medical assessment (triage) or operational requirement
    - This judgement may be made by medical staff or hospital management
- Assist hospital staff to transfer incoming patients by;
    - Clearing internal routes
    - Enforcing access zone rules
    - Directing vehicles through emergency drop off zones
- Be prepared to lock down the hospital

16.5. Infection control

Hospitals are unique in the way that they are a concentration point for possible infection and outbreak of disease. Hospital management will prepare strict policies to be followed by all staff in order to minimise the risk of infection and spread of disease.

16.5.1. General precautions to prevent spread of infection

Security staff working at a hospital must be aware of the basic principles of preventing infection.

Topic focus

Infection control measures at a hospital

1. **Hand hygiene**

Visibly dirty hands:

- Wash with soap and water
- Rub hands together for at least 15 seconds
- Rinse and dry with disposable towel
- Use towel to turn off water (if required)

Unsoiled hands:

- Rub with antibacterial rub
- Rub all surfaces of hands and fingers until dry
- Performed after
    - Contact with a person's skin
    - Contact with body fluids
    - Removing gloves
    - Handling phones, door knobs or other communal surfaces
    - Entering a new zone within the hospital

2. **Cough etiquette**
    - Cover mouth and nose with a tissue
    - Use the nearest rubbish bin to dispose of the tissue
    - Perform hand hygiene

    For patients or staff exhibiting coughing symptoms:
    - Offer face masks to reduce airborne spread of infectious droplets
    - Encourage dispersion of coughing personnel e.g. extra space around each person in waiting areas etc.

3. **Using PPE**
    If required to perform duties in a potentially infectious environment:
    - Wear a gown, covering torso from neck to knees
    - Wear a face mask
    - Wear sterile gloves
    - Dispose of all PPE after use in a medical waste container
    - Perform hand hygiene after disposal of PPE

4. **Airborne infection precautions**
    If a patient is suspected to be infected with airborne disease such as tuberculosis, measles or chickenpox:
    - Put a mask on the patient
    - Isolate the patient in the airborne infection isolation room (AIIR) or private room if no AIIR available
    - Restrict access to the room for people with low immunity e.g. have symptoms of illness
    - Restrict transport of patient unless medically necessary

5. **Textile and laundry handling**
    When hospital gowns and bedding have been used:
    - Ensure disposable patient gowns are placed in appropriate bins
    - Bedding linen is handled with minimum movement to prevent contamination of air, surfaces and people
    - Laundry is disposed of in approved chutes for collection and washing

16.6. Special considerations for hospital security

Security staff should be aware of special considerations for security at a hospital, and be prepared to act in an appropriate manner in order to maintain safety, security and public order within the hospital site.

16.6.1. Special patient types

There may be certain types of patient or visitor that could be classed as special, as they require a certain approach to handling or interactions, treatment, or protection. Such examples could include:

- VIPs
- Heavily drugged or under influence of alcohol
- Criminals under police custody
- Mentally disabled or genetic disorders e.g.
    - Alzheimer's
    - Dementia
    - Schizophrenia
- Unaccompanied children (no guardian found or available)

16.6.2. Special needs and people of determination

Security staff will likely encounter patients or visitors with special needs, and should be mindful of their requirements when moving within the hospital site. Simple acts of kindness such as holding a door or directing those in wheelchairs toward elevators or ramps can build a positive environment within the hospital.

Key information

Security staffs are not required to carry belongings, aide people to walk, or push wheel chairs – their primary duties are to the safety and security of people, property and information within the site. Arranging suitable help from hospital staff is sufficient, allowing Security staff to remain vigilant to risks and threats.

16.6.3. Empathy and discretion

Due to the emotions and stresses felt by all hospital users, including staff, patients and visitors, a key skill for Security staff is to display empathy and discretion. This approach to most situations can set the tone for a successful outcome to any personal grievance or complaint.

Most people entering a hospital are fearful, anxious and stressed no matter what their reason for being there, and a Security team who approach people with empathy can de-escalate stressful situations from the very beginning.

A tool commonly used by hospital staff is known as **HEART:**

- **H**ear the story (of the upset person)
- **E**mpathise with them
- **A**pologise for the fact they are upset
- **R**espond with suitable resolution options
- **T**hank them for their time and cooperation

Key information

Security staff working at a hospital will be exposed to many situations where they receive privileged information, and must display discretion in order to protect the confidentiality and dignity of others.

Figure 145 Empathizing with a frustrated patient

When greeting and welcoming visitors to the hospital facility, Security staff can follow the START method of customer service:

- **S**mile and greet
- **T**ell your name
- **A**ctively listen
- **R**apport and relationship building
- **T**hanking the person

This approach goes together with mindfulness of cultural considerations for patients, visitors and staff.

16.6.4. Patient confidentiality

Hospitals have an obligation to protect the personal information of patients, and there are very serious consequences to breach of patient confidentiality. Security staffs are in a position to support the hospital with maintaining confidentiality and through awareness, can prevent or reduce potential breaches. Examples of patient confidentiality breach may include:

- Theft of patient records
  - From wards, bedside, or filing areas
- Observation of patient condition, and disclosing this information to others
- I.T systems being breached
- Identity fraud
  - Criminals posing as hospital staff to obtain personal information about a patient

Figure 146 - Patient file confidentiality

Module 16 Revision

Revision questions

1. List 5 major security threats to hospitals

2. List 3 physical hazards present in a hospital

3. List 3 biological hazards present in a hospital

4. Describe the 3 main security zones of a hospital, giving 2 examples of what would be located in each zone

5. Recall the incident type for each code:

Code	Event
Amber	
Black	
Blue	
Brown	
Gold	
Green	
Grey	
Orange	
Pink	
Red	
Silver	
White	
Yellow	

6. List the 3 most common hospital incident types

7. Explain the code red evacuation procedure

8. List 4 examples of high security areas within a hospital

9. List 2 types of hospital user that would be authorised to enter a high security zone

10. List 3 times that hand hygiene must be performed

11. List 3 special patient types that a hospital may receive

12. Describe the principle of HEART when dealing with upset hospital patients, visitors or staff

13. List 3 examples of how patient confidentiality might be breached

Module 17
special events security

Module 17

Special event security

Qualification Link

Units

- Nil

Learning outcomes

1. Identify special event planning considerations
2. Identify roles of security at special events
3. List threats and hazards to special events
4. Outline incident response procedures
5. Recognise the impact of media perception and professionalism

Key definitions

Special event – A unique event involving a large gathering of people

Ticketing – Method by which entry to an event is authorised

Event management – Staff responsible for the organisation and logistics of the event

Sponsor – The organisation(s) that contribute funds toward running the event in exchange for public exposure and recognition

VOC – Venue operations centre, central control area for event operations and security monitoring

Figure 147 - Du Arena in Abu Dhabi

17.1. Introduction to special event security

Special events take place regularly within the UAE and the provision of effective security is essential to ensure the safety of all involved. A special event will typically involve a large team of Security staff, many of whom may not have worked together before, and various other personnel who will also contribute to the running of the event. Examples of special events may include:

- Concerts and musical performances
- Formula 1 racing
- Football games
- Food festivals
- Tennis tournaments
- Trade shows and conventions
- Cultural exhibitions

17.2. Roles and responsibilities of event security

Security staff working at a special event may be required to perform various roles and duties as part of a larger security team. Familiarisation with these roles will allow Security staff to contribute and offer flexibility to event security supervisors and managers.

17.2.1. Static posts

Locations that Security staff may be deployed to carry out duties at an event venue may include:

Pre-entry ticket checks

- Verify approaching spectators hold a ticket
- Direct spectators to the appropriate access control point

Security screening

- Personnel searches
- Vehicle search

Access control points

- Venue entry
  - Turnstile operator
  - Gate controller
- Vehicles
  - Delivery zones
  - Emergency vehicles
  - VIP arrivals
- Spectator zones
- Restricted zones

    - Performer or team areas
    - Venue infrastructure
        - Power & Utilities
        - Stairwells
    - Media zones
    - VIP and hospitality areas
- Parking and traffic management

Venue Operations Centre

- CCTV Operator
- Communications operator

Figure 148 - Automated turnstiles at a high security venue

17.2.2. Mobile duties

- Crowd monitoring
    - Crowd behaviour
    - Over crowding
    - Blocking of emergency escape routes
- Venue patrols
    - Inspection of critical security areas
    - Perimeter patrols
    - Parking areas
- Incident response teams
    - Crowd control
    - Evacuation guides
    - Additional support as required

17.3. Special event threats and hazards

Threats and hazards to a special event will depend on the type of event, venue, anticipated spectators and environmental conditions.

17.3.1. Threats to event security

Key information

Significant threats to event security may include:

- Fire
- Terrorism
    - Bomb threats
    - Suspicious devices
    - Person borne IED (Suicide vest)
    - Vehicle borne IED
    - Armed attack
- Crowd tension and violence
- Forced entry into the venue
- Protests or ideological demonstrations
- Crime outside and within the venue
- Alcohol and drug use
- Child abduction

17.3.2. Hazards at special events

Hazards present at an event will vary depending on many factors, however a basic guide to common special event hazards can include:

- Severe weather e.g.
    - Sand and dust storm
    - Extreme winds
    - Rain and flooding
- Structural failure e.g.
    - Seating collapse
    - Scaffolding and temporary structures
- Hazardous materials and substances e.g.
    - Pressurised cylinders
    - Flammable liquids and gasses
    - Landscaping supplies such as;
        - Fertiliser
        - Weed killer
    - Pest control poisons
    - Toilet waste
- Noise and vibration levels e.g.
    - Music concerts
    - Race tracks
    - Air shows
- Sun and heat exposure at outdoor events
- Fireworks and lasers

17.4. Screening and access control

Security screening and access control are primary duties of Security staff working at a

special event. The options and methods used to perform this task will vary depending on the type of event, venue and threat levels identified by the event planning team. For low security events such as a food festival in an open field, a simple visual search and ticket inspection may be sufficient. Other higher risk events may require detailed searching of personnel and belongings in order to ensure the safety and security of spectators attending.

IMAGES – Entry to an event

17.4.1. Visitor security screening

Topic focus

Security screening at venue Access Control Points

Security staff must check that:

- The person holds a valid ticket or venue ID
- The person does not possess any;
  - weapons or prohibited items/substances
  - Racist, offensive or political posters or banners
  - Alcohol or drugs
- The person is not under the influence of alcohol or drugs
- The person is permitted to access the zone or area using the ticket or ID presented

17.4.2. Access control methods

There are a variety of access control methods available for special events ranging from simple queues and visual ticket inspection, through to crowd distribution and automated turnstile systems. The methods and systems in use at each event will depend on the venue, and event type.

Key information

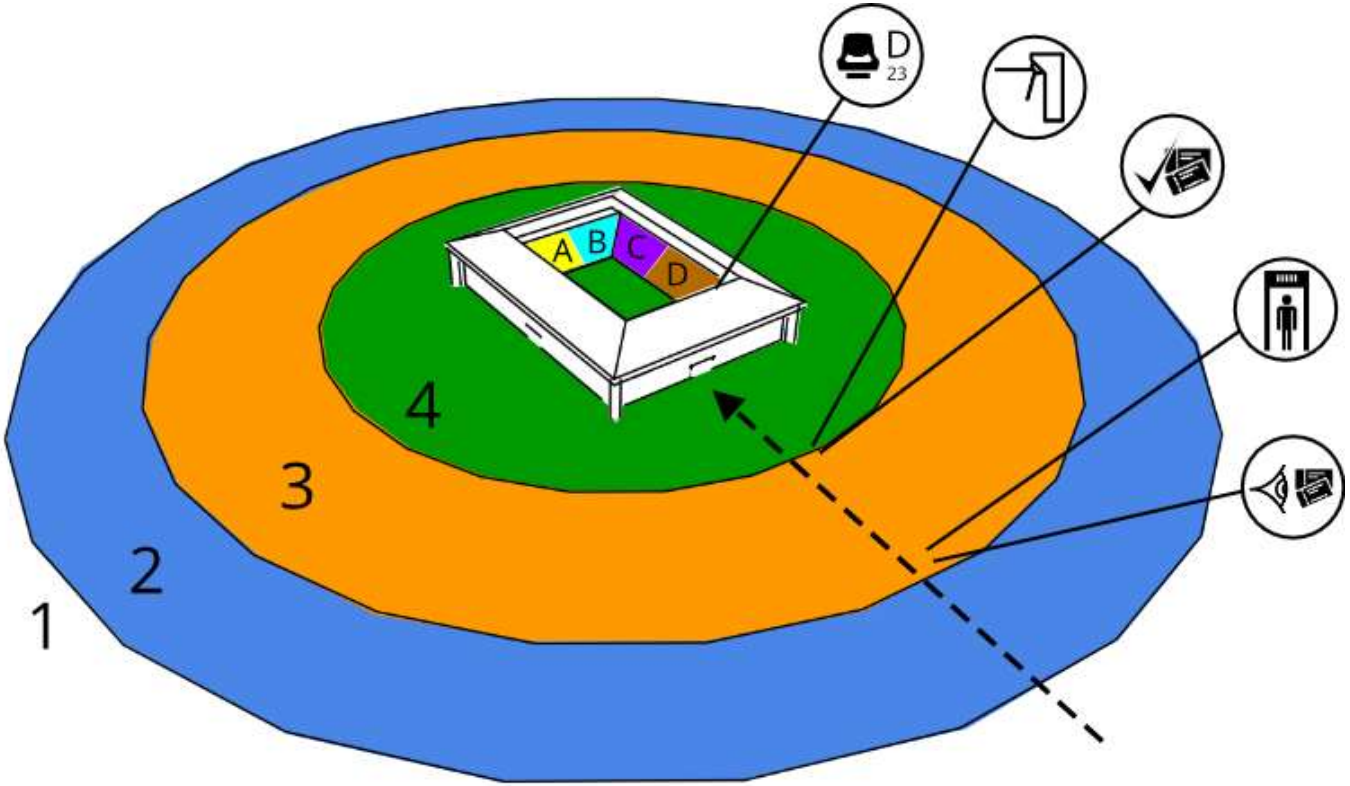
Venue signs

Well signposted approaches to the venue, along with clearly marked entry points for different viewing or seating areas can greatly assist with spectators regulating their own access into the venue, and reduce the load of Security staff to provide direction and control

A system of security zones can be used to define the limits of access for different ticket holders or venue ID holders. A recommended layout of zones for larger venues such as stadiums and concert halls is as follows:

- **Public zone** – Areas outside the control of event organisers and Security staff
- **Exclusive zone** – The approach to the venue where official ticket sales, merchandise or other promotional activities may take place
- **Outer perimeter** – First visual check of tickets and ID, along with a control line for security screening before entering the inner perimeter
- **Inner perimeter** – Entry turnstiles or gates where tickets or IDs are scanned and accounted for in official attendance counts, public access areas such as food and beverage outlets, toilets and smoking areas
- **Inner event zone** – Seating or spectator areas, divided according to ticket or ID held
- **Event participant zone** – Restricted to performers, teams, exhibitors and media. This zone can be further divided depending on the event, with specialised badges or ID used to control access to areas such as:
  - Backstage
  - Team rooms
  - Media and broadcast area
  - Venue Operations Centre
  - Operations offices, medical facilities, police and security facilities
  - VIP areas
  - Hospitality and catering preparation

An example of venue security zone layout can be found on the following page.



1. The public zone

2. The exclusive zone

3. The outer perimeter

4. The inner perimeter

Inner event zone – access granted as per ticket or ID accreditation

Figure 149 - Example security zone layout for larger event venue

Topic focus

Basic principles of controlling access to a venue for special events can be summarised as follows:

1. **Pre-entry**
    - **a.** Verification of tickets
    - **b.** Distribution of crowds into screening points
2. **Security screening**
    - **a.** Assessment of entry eligibility based on
        - **i.** Age
        - **ii.** State of mind (alcohol or drugs)
        - **iii.** Social behaviour
    - **b.** Search of people and bags
3. **Entry control**
    - **a.** Scanning or recording of tickets/ID
    - **b.** Movement through turnstile or gate into inner perimeter
4. **Spectator placement**
    - **a.** Movement from inner perimeter to inner event zone based on ticket privileges
    - **b.** Enforcement of seating and zones

Safety!

The points of entry to large venues may present a serious risk of crowd crushing, or breach of access control points if consideration is not given to the design and layout of approaches in the outer perimeter.

A method of delaying and distributing crowds as they approach should be considered such as the use of zigzagging approach routes

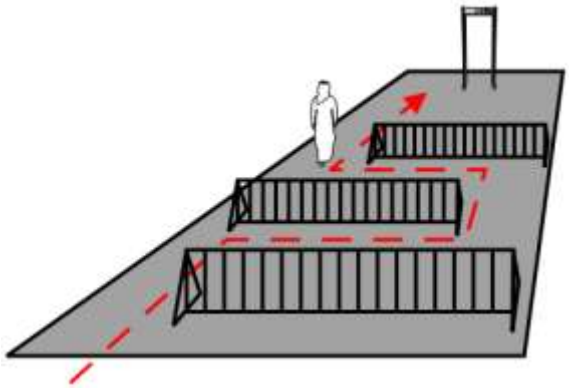


Figure 150 - Distribution of arriving spectators through zigzagging approach to ACP

17.4.3. Parking and traffic management

Security staff may work together with other event staff to coordinate traffic entering the venue parking. The principles of traffic management and directing vehicles will still apply, however there may be several additional factors that require consideration.

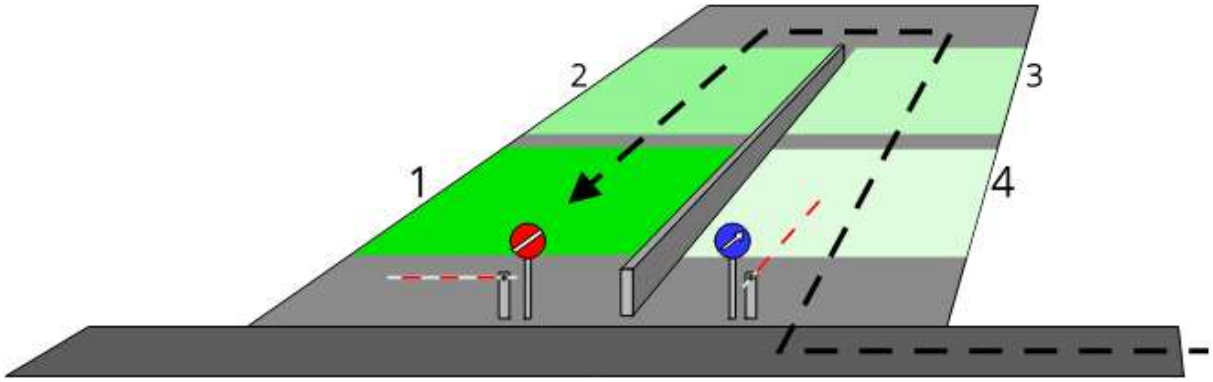
Depending on the event venue, its location within a city, number of vehicles attending and space available for parking, the following may be required:

- Street closures in the surrounding area
    - Permissions from municipality
    - Coordinated by police
- Sign posting directing approaching vehicles into allocated parking areas
- Specific parking entry and exit points
    - Reduces congestion if traffic flows in and out through different points
- Parking space indicators
    - Spaces available
    - Sections closed off until required

Safety!

Security staff performing parking and traffic management duties must maintain personal safety through the use of appropriate PPE including:

- High visibility vest
- Traffic direction wands
- Torch



- Parking management requires arriving spectators to fill parking spaces from furthest point into the parking lot
- Separate entry and exit points to increase traffic flow

Figure 151 - Parking area layout and flow

17.5. Security team resources

Security staff working at a special event must have access to sufficient resources and instructions in order to carry out their duties effectively. Event management, security managers, and emergency departments will need to ensure that appropriate plans and tools are available to Security staff.

17.5.1. Required plans and resources

In order to effectively provide prevention and response capabilities at a special event, Security staff must be able to access:

- Contact numbers for key personnel
- Venue maps identifying;
  - Seating or viewing zones
  - Restricted areas
- Site security plans identifying;
  - CCTV locations
  - Zone boundaries
  - Entry and Exit control points
  - Medical treatment points
  - Evacuation routes
  - Safe assembly points
  - Static post duty locations
- Contingency plans for identified incident response e.g.
  - Evacuation
  - Lost child
  - Crowd violence
- Codes of conduct for spectators
  - Prohibited items
  - Acceptable behaviour
  - Removal from venue

17.6. Incident response

As with any safety or security incident, Security staff must assess the potential for harm to people or property, and respond in an appropriate manner. Before any event, Security staff and other key staff working at the venue will need to conduct training and rehearsals for incident response.

Topic focus

Agencies operating at special events

Security staff will need to be familiar with, and cooperate with the follow agencies commonly present at special events:

- Police, including traffic control
- Ambulance services
- Civil Defence
- Venue owners
- Event management staff

Key information

It is important that event staff and Security teams rehearse incident response at the specific venue hosting the event in order to provide familiarity and awareness to personnel that may not have worked together, or at that particular venue before.

17.6.1. Common incidents at special events

Some incidents that are common at special events may include:

- Lost and found items
- Minor first aid
- Lost child reported

- Lost child found
- Prohibited items detected at Access Control Point
- Spectator seated in wrong location
- Lost or stolen tickets
- Illegal ticket sales outside the venue

17.6.2. Critical incidents at special events

Examples of critical safety or security incidents at special events include:

- Fire
- Terrorist attack
- Power failure
- Gas leaks or hazardous material spills
- Security system failure e.g.
    - Automated turnstiles
    - CCTV
    - PA systems
    - Fire warning and detection systems
- Stage, pitch or performance zone invasion
- Crowd crushing or panic
- Natural disasters e.g.
    - Flooding
    - Extreme winds
    - Lightning strikes
    - Earthquakes

Key information

If a venue is large and holds many visitors, an evacuation may need to be conducted in sections. Security staff should be prepared to coordinate evacuation section by section under control of the Event Security Manager.

17.7. Media perception and professionalism

Most events will have some form of media coverage, and members of the media may be granted special access to zones within the venue. Security staff should be familiar with the credentials required to identify members of the media, what access privileges they are given and what equipment they can carry.

17.7.1. Media at special events

The presence of media at events means that if any safety or security incident occurs, it will almost certainly be noticed and captured by the media. Security staff must remain aware of this, and respond in a professional and ethical manner. Examples of unprofessional behaviour include:

- Inappropriate searching procedures
- Intimidation of spectators
- Inappropriate use of force
- Accepting bribes
- Allowing access to zones without proper tickets or ID
- Confiscating items that are not prohibited

Key information

The consequences of poor security practices being broadcast by media may include:

- Legal action against negligent Security staff
- Damaged reputation of event organisers
- Financial loss due to withdrawal of event sponsorship

17.7.2. Professionalism in the public environment

Security staff working at special events are exposed to a large number of agencies and members of the public, and must represent their organisation with professionalism. The basic standards of personal presentation must be met, and a calm and confident approach to duties will encourage event spectators and staff to follow directions and cooperate with Security staff. A professional image presented to the public may:

- Encourage cooperation
- Discourage potential criminals
- Increase event organiser confidence, resulting in future business for Security organisations

Figure 152 - Professional image while on duty

Module 17 Revision

Revision questions

1. Identify 5 Major security threats to special events

2. List 3 Major health hazards that could be present at a special event

3. List 5 Static Post roles of security at special events

4. List 3 Mobile post roles of security at special events

5. Explain why it is important for event staff and Security to rehearse incident response

6. List 3 common incidents that occur at special events

7. List 3 Major incidents that might occur at a special event

8. Describe what might be required to successfully evacuate a large venue with many people

9. List 3 behaviours that Security staff should avoid that may result in negative media coverage

Module 18
Ports, Airports, and land borders security

Module 18

Ports, Airports and Land borders security

Qualification Link

Units

- Nil

Learning outcomes

1. Identify unique considerations for sea port security
2. Identify unique considerations for airport security
3. Identify unique considerations for land border security
4. List specific threats and hazards to Ports, Airports and Land borders
5. Outline systems of control used at national borders
6. Identify organisations and agencies working at national borders
7. Identify methods of access control within national border checkpoints
8. Outline vehicle movement procedures while airside at an airport
9. Outline incident response procedures for Ports, Airports and Land borders

Key definitions

Security alert level – A system of categorising alert levels in accordance with heightened risks of security threats, Level 1 – Level 2 – Level 3

Port – A geographical area located by the sea for the logistics of maritime transport

PFSO – Port Facility Security Officer, the person in charge of port security operations

Airport – A geographical area designed to accommodate aircraft, passengers, cargo and maintenance operations

ATC – Air Traffic Control tower responsible for guidance of all aircraft using the airport

Airside – The sector of the airport in which aircraft move e.g. runways, taxiways, hangars and aprons

Land border – The agreed physical line between 2 or more nations

National border – The point at which a person is processed into a country e.g. airport, port, land border

Customs – The government agency responsible for the protection of a country through regulation of incoming goods and people

18.1. Introduction to National border security

UAE National borders provide a barrier of protection for citizens and residents from external risks and threats. Government policies regarding immigration, import and export are enforced at National borders in order to provide National Security. Security staff may work alongside other public security agencies to achieve the National Security mission of the UAE.

18.2. Port security

Port security is concerned with the safety and security of operations at maritime ports. Security staff will often be deployed to provide protection to people, property and information at a port, and should be familiar with specific threats and hazards at ports, and systems of providing security.

Figure 153 - Complex security environment of a port

18.2.1. Sea Port security threats

Security breaches at a sea port can result in serious consequences, from small theft all the way up to deliberate sabotage of critical facilities within the port such as container cranes and warehousing.

Key information

Specific security threats at ports may include:

- Stowaways and illegal immigrants
- Theft of cargo during loading and unloading
- Smuggling of drugs, weapons or other

prohibited items
- Hazardous materials transport
- Terrorist attacks
- Organised crime rings
- Importation of radiological (dirty) or biological weapons

18.2.2. Sea Port hazards

Key information

Specific safety hazards at sea ports include:

- Container loading and unloading
  - Crush or impact hazards
  - Overhead cargo loads
- Slips and trips on cabling, ropes and wet surfaces
- Falling off docks into water
- Spillage of oils and petrol (flammable)
- Noise and vibration of heavy machinery
- Shared space with vehicles and plant machinery

18.2.3. Organisations and Agencies operating at Sea Ports

Security staff should be aware of the other agencies and organisations working at the port, and what their role is in relation to port operations. Typical agencies working at a port include:

Ministry of Climate Change and Environment (MOCCAE)

- Supporting biosafety within UAE by protecting from importation of unsafe foods, animal or agricultural products
- Protecting against epidemics and disease

Abu Dhabi Food Control Authority (ADFCA)

- Ensuring health of animals and plants entering the UAE

Critical Infrastructure and Coastal Protection Authority (CICPA)

- Safeguarding the coastal waters surrounding ports, and critical infrastructure sites

UAE Federal Customs Authority (FCA)

- Facilitating the movements of trade and passengers through a port
- Inspection of goods and materials

Civil Defence

- Responding to fires
- Supporting incident management and disaster recovery

Other port users

- Seamen
- Navy crews
- Port operations staff

18.2.4. Systems of security control within Sea Ports

Like most large sites, sea ports utilise a variety of systems to control security in and around the port. Common systems include:

- Access Control Points at the entrance to ports
- Security zones within the port site
  - Entry control at transitions between zones e.g. RFID card, Padlocks etc.
- CCTV and control rooms
- Container and cargo inspection and searching
- Vehicle and personnel searching

Topic focus

Static guarding duties at a port

General duties:

- Supervise parking areas outside the main port entrances
- Inspect trucks and light vehicles for authorised personnel and cargo
- Foot patrolling of various security areas within the port
- Clearance of passenger terminals after last ship or ferry departs
- Escort and monitoring of work crews on site at the port, including verification of permits to work
- Direct and guide external agencies such as Police and CID to the appropriate locations
- Report and record health and safety incidents and near misses
- Inspection of port ID for incoming personnel and vehicles

- Completion of port visitor and contractor logs
- Liaise with the control room in event of emergencies
- Opening and closing of daily use facilities e.g.
    - Office and administration areas
    - Training facilities
- Inspection of cruise ship ID for passengers coming on board or departing the ship
- Vehicle patrols of port facilities
- Control room duties including radio operator, CCTV operator and key holding
- Reporting and recording incidents and occurrences in the daily occurrence book

18.2.5. Incident response

Due to the critical nature of ports, most security incidents will be responded to by Police and other supporting agencies. In the event of a serious incident, Security staff will respond as per the local site standard operating procedures, and be prepared to cooperate with public security agencies and civil defence.

Examples of critical incidents may include:

- Fire
- Capsized vessel
- Container crane collapse
- Release of hazardous materials
- Serious vehicle accident
- Suspected improvised explosive device (IED)
- Armed robbery

18.3. Airport security

Security staff may be deployed to airports to provide safety and protective services to airport staff, passengers, assets and procedures. Airport security is regulated by several international conventions and codes of practice, along with local policies and practices, and Security staff should be aware of these regulations for both compliance purposes and to enable effective provision of security services.

Airports and airlines are a high value target for potential threats as they represent national capabilities, well developed societies, and are essential to economic stability, along with receiving widespread media coverage should any incident occur. Targeting an airport can cause serious disruption to a country through both financial and reputational loss.

Key definitions

ICAO – International Civil Aviation Organisation

IATA – International Air Transport Association

ACI – Airports Council International

Figure 154 - Complex security environment of an airport

18.3.1. Aviation security threats and risks

Key information

Specific threats to airport safety and security may include:

- Terrorism
- Sabotage
- Theft and organised crime
- Insider threats
- Cyber and I.T Network attacks

18.3.2. Aviation hazards

Airports are large and complex sites with many areas that can present hazards to those working and travelling.

Safety!

Health and safety considerations whilst airside include:

- Extreme noise
- Moving vehicles
- Aircraft engine exhaust
- Fume inhalation

18.3.3. Airport security operations

Security is achieved at airports through a system of access zones, security clearance requirements for different employees and staff, and technologies.

Airports are divided into security zones and access is controlled through a variety of measures including:

- Wearing of ID
- Access cards for doors
- Keys and locks

The security of an airport is shared between several agencies and organisations, and commonly will include:

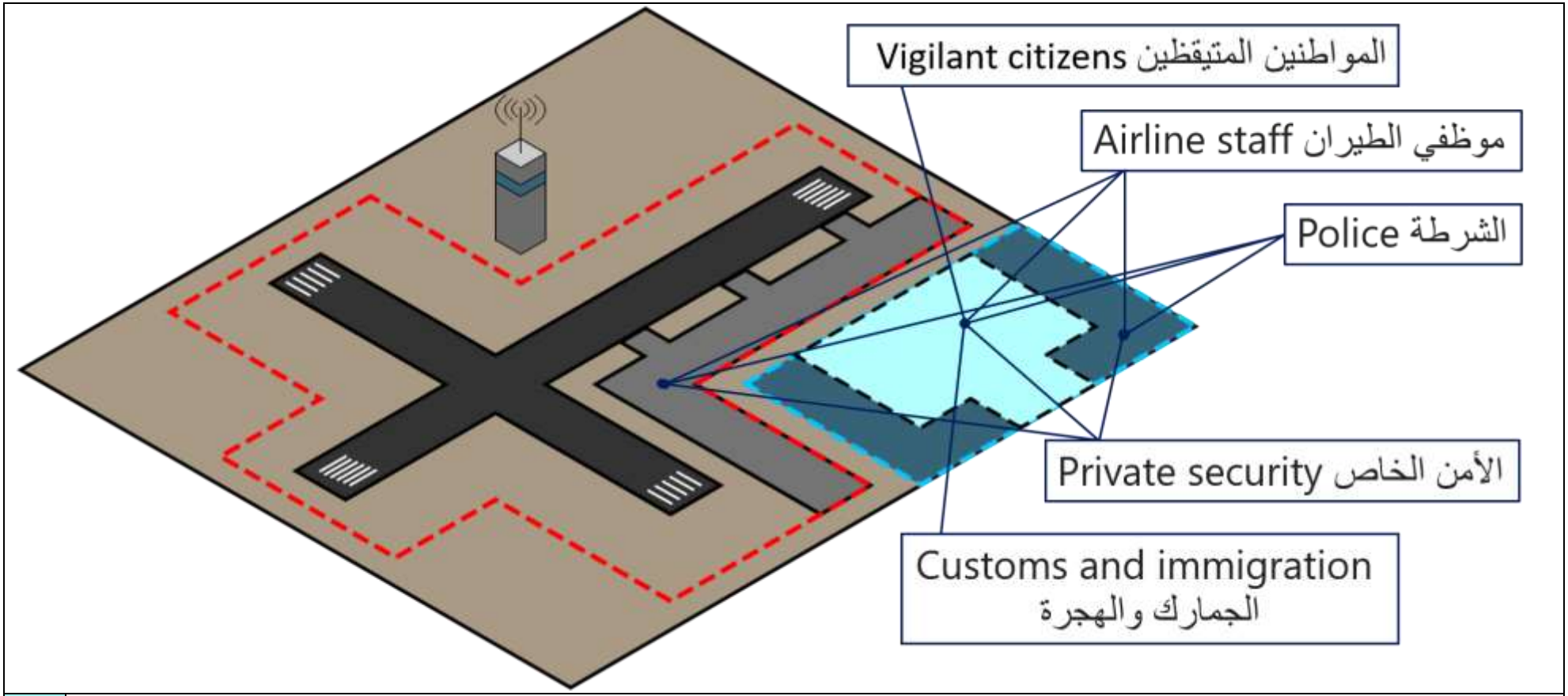
- Police
- Airline staff
- Customs and immigration
- Private security
- Vigilant citizens

Security zones can be divided into:

- **Airside** – the area that aircraft and supporting machines and equipment operate, e.g. runway, tarmac, baggage loading and fuelling trucks
- **Terminal** – The check in, immigration and security screening, and departure or arrival lounges

Within these 2 major zones, an airport may be divided into further security zones with different levels of access control. Security staff must be aware of the access control measures, and authorised personnel at the airport.

Example of Airport Security agencies and their areas of operation



18.3.3.1. Passenger and baggage inspection

One of the most important security measures at an airport is the inspection of passengers and their baggage. This process is normally carried out by customs officials, however private security staff may be required to assist, and should be aware of the passenger screening process.

Topic focus

Passenger inspection is normally divided into 3 components, that each have several considerations including:

1. **Checkpoint entry**
   a) Pre-inspection and queue zone
   b) Bag unpack and inspection zone
2. **Inspection point**
3. **Repacking zone**
   a) Seating and tables for repacking
   b) Inspection tray return

Security staff may be required to direct passengers through each of these zones, and assist customs staff with secondary inspection of suspicious items, perform searches of people or maintain an orderly queue and flow of passengers.

Duties at the checkpoint entry include:

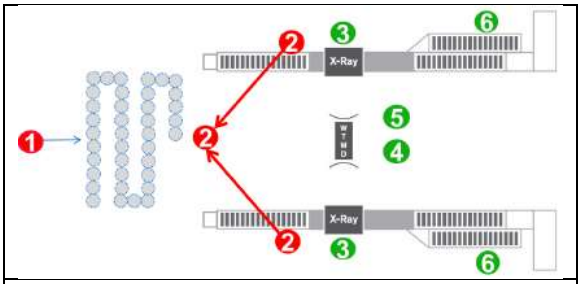
- Direction of passengers through the queuing area
- Notifying passengers of security rules and regulations
- Assisting passengers to arrange their belongings on the x-ray tray
- Looking for suspicious people or items

Duties at the Inspection point include:

- X-Ray operation and inspection
- Walk Through Metal Detector
- Physical searching of people
- Secondary searching of bags
- Explosive or narcotics trace detection

Duties at the repacking zone include:

- Return of inspection trays
- Looking for suspicious activity



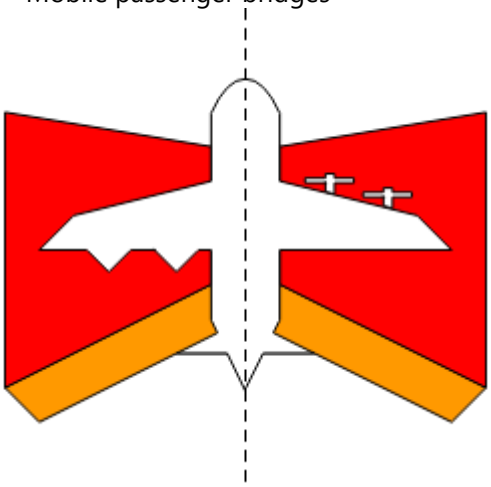
1. Queue supervisor for busy periods
2. Tray loader for x-ray inspection
3. X-ray operator
4. Male searcher
5. Female searcher
6. Secondary searchers for suspicious bags

Table 20 - Example of security staff duties at Airport inspection point

18.3.3.2. Aircraft security

Aircraft security is very important, as the aircraft represent a valuable target for attackers. Security staff may be required to provide physical security for aircraft that are parked on the tarmac during refuelling, passenger loading or unloading, and baggage handling procedures. Some important considerations for security staff include:

- Health and safety around aircraft
  - Noise
  - Jet engine exhaust
  - Propellers
- Safe distances from the aircraft
- Routes that support vehicles are travelling on e.g. refuel trucks, baggage trucks etc.
- Mobile passenger bridges



	Critical danger of propellers and jet engines
	Hazard of moving vehicles accessing the aircraft

Figure 155 - Example of aircraft dangers

Key information

If an attacker is able to access non-passenger areas of an aircraft, very serious damage and death may be possible through sabotage, deliberate damage or other interference with the aircraft.

Aviation security is a specialist field, and some Security staff will spend their careers developing additional skills and knowledge in this area. The threats and risks are constantly changing, and new methods of security and prevention are developed.

18.4. Land border security

Land border security is the protection against threats to the national interests and society of the UAE. Countries around the world maintain the right to protect borders, and Security staff should be aware of the types of threats, risks and systems of security control used at land border crossing points.

18.4.1. Land border security threats

Key information

Threats to the security of land borders can be categorised into the following types:

People or groups who wish to harm the UAE

- Terrorists
- Political activists

Criminals

- Smuggling
- Illegal or prohibited item trafficking
- Counterfeit goods

Unauthorised migrants

- Seeking a new life
- Running from trouble
- May bring antisocial behaviours into UAE society

The threats categorised here may present a variety of risks to security and safety, including the potential for:

- Explosive events e.g. bomb threats and IEDs
- Armed attack
- Hostage taking
- Unarmed violence e.g. physical assault

18.4.2. Land border security hazards

The types of hazards present at land border crossing points will depend on the infrastructure and facilities, location, and equipment or machinery present, however some potential hazards may include:

- Environmental exposure at outdoor inspection points e.g.
  - Sun burn
  - Heat stroke
  - Dehydration
  - Sand and dust
- Vehicles and traffic
  - Impact and crush injuries
  - Pinching or cutting of hands while performing search duties
  - Noise exposure
  - Fumes and gas inhalation
- Biological hazards e.g.
  - Interaction with animals and animal waste
  - Agricultural products and materials
  - People immigrating across the border may carry illness or infection
- Fuel, oil and flammable liquids stored on site
- Radiation exposure through X-Ray inspection

Figure 156 - OHS Hazards as trucks queue to enter border control point

Figure 157 - Border crossing point - UAE & Oman

18.4.3. Systems of security control at land borders

Security staff deployed at land border control points may be required to support a variety of agencies in the performance of their duties, including customs officials, police, military and operations staff.

A familiar idea of security access control zones can be applied to border control points with the following zones identified:

- **The approach zone**
- **The access control zone**
- **The response zone**

Topic focus

The actual procedures followed will depend on the policies and directives for each border crossing point, however, a typical land border crossing point may be operated in the following way.

The approach zone

Incoming traffic control:

- Divided at the earliest opportunity into 4 categories:
  - Pedestrians
  - Light vehicles
  - Coaches and buses
  - Cargo transport
- Coaches, and cargo transport vehicles are diverted to heavy vehicle inspection lanes
- Pedestrians are directed to proceed toward customs and immigration area
- Light vehicles are directed through inspection lanes

The access control zone

Security screening:

- Drivers are directed to position their vehicles in the appropriate inspection bay
- Passengers and other personnel are directed into customs and immigration area
- Visas, permits and documentation are inspected or issued by customs officials
- Men and women are separated for personal and belongings search according to policies

Vehicle and cargo inspection:

- Vehicles are passed through x-ray inspection points if available
- Cargo is passed through x-ray inspection
- Luggage and vehicle compartments are searched as required by policy
- Import or export permits and paperwork is checked for cargo loads
- Drivers and passengers return to vehicles for onward movement

The response zone

Progression through the border control point:

- Customs and immigration cleared personnel collect security screened personal possessions
- Vehicles are directed forward and out of the access control zone and into the response zone (inside UAE)
- A secondary line of control is available to delay unauthorised access into the country e.g.

    - Police unit
    - Additional barriers
    - Extended area of empty space allowing police or military intervention before offenders arrive at towns or cities
- Patrols may be conducted along the border line to detect unauthorised crossings

Security staff may perform various duties within the system of security control including:

- Traffic control
- Personnel and vehicle security searches
- Assisting customs officials
- Inspecting IDs and documents
- Preventing unauthorised access to security controlled areas
- Ensuring personnel and vehicles are matched correctly after screening
- Controlling all movements of persons in transit within the border control point

1. Traffic controller
2. CCTV/Detection tools
3. Hostile vehicle barriers
4. Border fencing
5. Light vehicle search
6. Access control breach response (police, barriers etc.)
7. Bags and belongings search
8. Personnel search
9. Customs and immigration
10. Heavy vehicle search

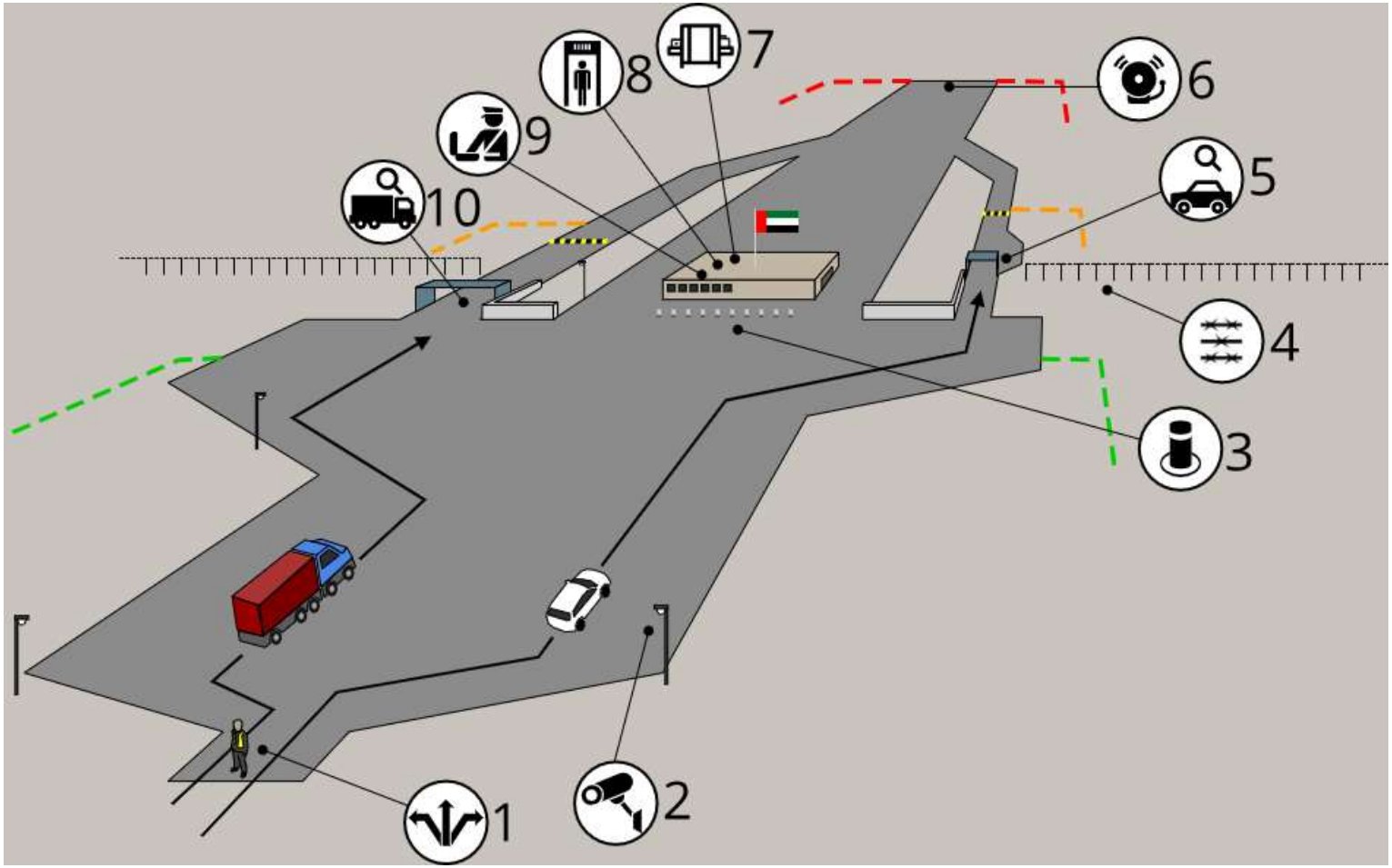


Figure 158 - National border crossing point

Module 18 Revision

Revision questions

1. List 3 threats to port security

2. List 3 hazards at a port

3. List 3 threats to airport security

4. List 3 hazards to health at an airport

5. What are the 3 components of airport passenger screening

6. Name 4 agencies working at an airport that contribute to security

7. List 3 organisations that work at a port

8. What is the IATA

9. What is the ICAO

10. List 3 security threats to national land borders

Module 19
Critical infrastructure

Module 19

Critical Infrastructure

Qualification Link

Units

- Nil

Learning outcomes

1. Define what is critical infrastructure
2. Identify critical infrastructure threats risks and hazards
3. Outline standard security measures implemented at critical infrastructure sites
4. Outline incident response procedures for most common incident types
5. Outline incident response procedures for most dangerous incident types

Key definitions

Critical infrastructure – Assets that are essential for the functioning of society and the economy

Desalination – The removal of salt and minerals from salt water in order to make it drinkable

Power generation – The production of electricity from sources of energy such as oil, gas or nuclear reactors

19.1. What is critical infrastructure?

Critical National Infrastructure, is facilities or assets that provide essential services or utilities for a society and economy to operate. Critical Infrastructure can be found across many industrial sectors including communications, defence, emergency services, public transportation and energy. This section will focus on the security of critical infrastructure in the energy and water systems sectors.

Examples of critical infrastructure facilities include:

- Nuclear power plants
- Oil and Gas
    - Extraction sites
    - Transport pipelines
    - Storage and distribution facilities
- Electrical grid distribution stations
- Water treatment and desalination facilities

19.2. Nuclear infrastructure security

Nuclear energy can be used to provide power to a nation, and the disruption of operations may result in serious harmful consequences through the loss of power supply. The nuclear materials used to generate power are also highly controlled, and the theft or smuggling of these materials is a critical incident that must be guarded against.

19.2.1. Nuclear security regulation

The UAE Government has established Federal Law no. 6 of 2009 Regarding the peaceful uses of nuclear energy, and formed the Federal Authority for Nuclear Regulation (FANR) to oversee the activities of nuclear energy in the UAE.

Responsibilities of FANR include:

- Issuing licences to operate in the nuclear energy sector
- Setting radiation dose exposure limits
- Optimising radiation protection in nuclear facilities
- Regulating the design of nuclear power plants
- Regulating the physical protection measures for nuclear material and facilities
- Emergency planning and preparedness for nuclear facilities
- Regulating safe transport of radioactive materials
- Conducting inspections and studies ensuring compliance with regulations

The UAE is also signed up to the International Atomic Energy Agency – IAEA, and follows global standards on Nuclear safety and security including the treaty on the non-proliferation of nuclear weapons

19.2.2. Nuclear safety hazards

Health and safety risks at a Nuclear energy producing facility will be similar to other industrial facilities except for one major area. Radiation exposure is the single greatest health risk to Staff working at a Nuclear energy site.

Radioactive materials

- Naturally occurring metals from the earth
- Used to fuel Nuclear reactors
- Used in medical equipment
- Can be found in small amounts in common items including:
    - Smoke detectors
    - Bananas
    - Brazil nuts

Ionising radiation

- Energy transmitted with enough energy to change physical matter
- Can come in safe levels such as
    - Rays of the sun
    - Medical x-ray
    - Natural levels in the earths soil
- Exposure to radiation is called a 'Dose'
- Dose is measured in 'Millirems'
- Most humans receive a dose of 280 millirems per year from natural sources

When working at a Nuclear Energy Plant, there are many safety barriers to limit the amount of radiation dose that staff are exposed to. Three simple principles are:

- **Create a barrier** – Steel, concrete and water provide protection from radiation. The Nuclear reactor inside an energy plant will have several layers of thick walls made of steel and concrete
- **Minimise time** – The less time a person spends near a radiation source, the smaller dose they will receive
- **Increase distance** – The further away a person is from a radiation source, the smaller dose they will receive

Security staff may be exposed to low levels of radiation while on duty, and will be required to wear a badge called a dosimeter that measures how much radiation dose they are exposed to.

19.2.3. Nuclear security threats

The biggest threats to nuclear security is the illegal smuggling of radioactive materials. These can be used to build weapons, and cause massive harm.

Topic focus

Security staff will inspect all vehicles and people entering and leaving a Nuclear Energy Plant. Detection of radioactive material can be done using 3 types of detector:

Pocket detecting device

- Used to detect radiation levels

Hand held detector

- Used to detect, locate the position, and measure dose levels

Automatic detector

- Used to detect radioactive material within goods, baggage, cars and trucks
- When using the detectors, they should be calibrated and the alarms set to the appropriate radiation level to avoid false alarms
- Security staff will use the Hand held detector to conduct inspections when entering or exiting a nuclear power plant

Figure 159 - Barakah Nuclear Power Plant, UAE

19.2.4. Nuclear critical incident response

Nuclear Power Plants will plan and rehearse critical incident response with the Regulatory Authority (FANR) and other organisations such as the police, civil defence and military. Security staff working at a Nuclear site will be required to participate in incident response drills and understand the requirements that they must fulfil.

The details of these plans are kept secret on a need to know basis, and only Staff who have been cleared to work at these sites will receive the relevant response plans.

19.3. Oil and Gas plant security

The UAE has major Oil and Gas production facilities, and disruption to these operations can cause major financial loss, and potential destabilisation of the economy and society.

The provision of physical security is essential to safeguard against acts of sabotage or terrorism, and accidents or safety breaches.

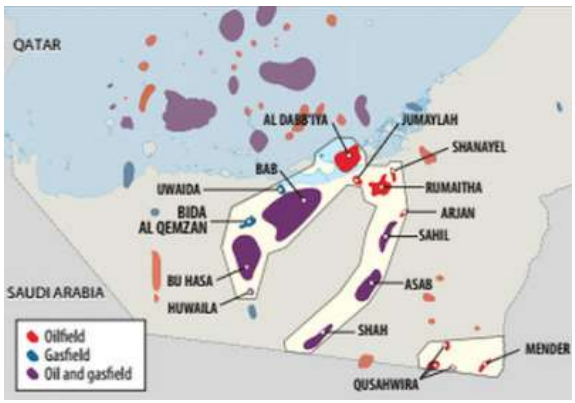


Figure 160 - Map of Abu Dhabi Oil and Gas fields

19.3.1. Oil and Gas safety hazards

Within oil and gas extraction, transport and refinery facilities there are many health and safety hazards. Some prominent hazards may include:

- Explosion and fires
- Vehicle collisions
- High pressure pipes and equipment
- Falls from platforms and raised walking paths
- Noise and vibration of operating equipment

Safety!

When working in high risk areas, Security staff must observe the PPE requirements and wear the protective equipment as appropriate

Figure 161 - Facility in Abu Dhabi, UAE

19.3.2. Oil and Gas Security threats

Oil and gas security threats may come from a variety of sources, and these threats will be monitored by National Security agencies and reported to the relevant organisations for better awareness.

Figure 162 - Burning oil wells in northern Iraq after sabotage by terrorists

Topic focus

As with most other sites, the means to protect oil and gas facilities can be achieved through the use of the 4 D's

- **Deter**
- **Detect**
- **Deny**
- **Delay**

These principles applied to an oil or gas site with the related technologies and monitoring systems will provide a level of protection that will allow time for Public security forces such as the police or military to respond to major breaches of security.

19.3.3. Oil and Gas critical incident response

High risk / critical incidents planned for at Oil and Gas sites include:

- Fire or explosion
- Suspicious or confirmed explosive device
- Gas leak / Oil spill

Sites will prepare response plans for specific incidents and all staff will be involved in the rehearsal and practice of these plans.

19.4. Water treatment and desalination

The UAE relies on desalinated water for drinking, and this process is done 70 major desalination plants along the UAE coastline. There are also several dams constructed throughout the emirates to store rainwater for use in agriculture and other industries.

Any disruption to water treatment and storage will produce serious and costly consequences, and may have a large impact on the economic and social stability of the UAE.

19.4.1. Water treatment facilities safety hazards

The most serious hazards to health and safety at water treatment facilities include:

- Electrical transformers overheating causing fire
- Leakage of treatment chemicals
- Explosion of high pressure pumps

These hazards can be controlled through regular inspection of equipment and servicing; however, this responsibility will fall to other departments within the organisation. Security staff should report any observations that may offer clues to equipment becoming worn or unsafe.

Figure 163 - Taweelah water desalination plant , UAE

19.4.2. Water treatment security threats

Threats to security at water treatment facilities may include:

- Terrorism
- Political enemies
- Disgruntled employees
- Unsupervised visitors or contractors

Topic focus

Security staff will be required to maintain safety and security through applying:

- Access control
- Patrolling
- Monitoring and inspection of high security areas
- Reporting and follow up of incidents

Water treatment facilities are vital to the continued stability of UAE society, and they must be protected as high priority. Security staff will contribute to the overall security plan for these sites and must be prepared to learn about the complex issues in such vital facilities .

Module 19 Revision

Revision questions

1. Name the regulatory agency for Nuclear Power in the UAE

2. Identify the major health hazard at Nuclear Power Plants

3. Describe how security staff will prevent the unauthorised removal of radioactive materials from a Nuclear site

4. Name the device that measures the dose of radiation a person receives when working at a Nuclear site

5. List 3 devices used to detect radioactive material

6. List 3 major hazards at oil and gas facilities

7. Identify 2 critical incidents that could happen at an oil and gas facility

8. List 4 potential security threats to water treatment facilities

Module 20
Museum and cultural centre security

Module 20

Museum and Cultural Centre security

Qualification Link

Units

- Nil

Learning outcomes

1. Identify unique threat, risk and hazard considerations for museums and cultural centres
2. Outline security control options for use at museums and cultural centres
3. Outline response procedures for critical incidents at museums and cultural centres

Key definitions

Cultural centre – A place designed to exhibit cultural practices, traditions and history

Museum – A place devoted to the procurement, care study and display of objects of lasting interest and value

Artefact – An object made by humans of historical or cultural significance

Counterfeit – An object made in imitation of an original, attempting to be passed as a genuine article

Figure 164 - Sharjah museum of Islamic Civilization

20.1. Introduction to Museums and Cultural Centres

The UAE has a wide range of museums and cultural centres, with many high profile and rare artefacts on exhibit. There are items of priceless and irreplaceable value, along with cultures and customs on display for the world to view. The security of these establishments is a serious task, and Security staff may be asked to perform various duties in providing for the safety and security of people, property and information at these establishments.

Key information

Prominent museums and cultural centres in UAE include:

- The Louvre Abu Dhabi
- Dubai Museum
- Sharjah Museum of Islamic Civilisation
- Al Ain National Museum
- Sheikh Zayed Palace Museum

20.2. Unique security risks and threats

Museums and cultural centres offer attractive targets for theft and often the biggest threat can come from insiders working within the organisation. Security staff must be aware of any changes to behaviour and suspicious activity from within, as well as any external threats such as:

- Potential surveillance
- Attempts at bribing of staff
- Attempts to damage exhibits
- Unauthorised handling of exhibits by visitors
- Unauthorised photography

20.2.1. Historical importance

Many exhibits at museums or cultural centres can be considered priceless as they hold historical importance and cannot be replaced if stolen or damaged. This places an extra level of responsibility on Security staff to ensure that the historical record of exhibits and antiquities are preserved for future generations.

20.2.2. Handling of artefacts and antiquities

Specially trained museum staff will be permitted to handle artefacts and antiquities, and Security staff should not attempt to do so. There is the potential for even the slightest interference

from untrained people to cause damage to artefacts.

If exhibits are being transported in or out of a museum or cultural centre, Security staff may be involved in providing a secure route for the loading and unloading of exhibits. In this case, the items should be treated as any other valuable asset and due care given to the protection of those items.

20.2.3. Theft

Theft is a constant threat, and Security staff must be vigilant to the possibility of theft occurring. It is normal for museums and cultural centres to use several layers of security systems and technologies to protect against theft, and these options will be noted in the following section.

20.2.4. Counterfeit

Potential thieves or other organised crime rings may attempt to replace genuine exhibits with counterfeit copies, and these will normally be detected by specialists from that field. Security staff should be aware of any suspicious activity around the transfer of exhibits that may indicate swapping or replacement of genuine exhibits with counterfeit copies.

20.2.5. Wilful damage

There may be occasions where a visitor or member of staff attempts to cause damage to exhibits or items of cultural significance. This may be due to:

- Political or social disagreements
- Disgruntled employment
- Juvenile behaviour

Security staff should be aware of any person carrying the means to cause damage, or behaving in a way that the intent to cause damage is suspected.

20.2.6. Sources of risk at Museums and Cultural Centres

Aside from direct threats such as theft, damage and counterfeit exhibits, there are further sources of risk such as:

- Damage caused by environmental conditions e.g.
  - Dust/Sand
  - UV Exposure (Sun light)
  - Damp or Dry air
- Fire
- Exposure to cleaning agents or chemicals

Security staff can play a part by being aware of potentially damaging conditions and reporting these to the appropriate departments within the museum or cultural centre.

20.3. Museum and Cultural Centre security options

Topic focus

Applicable security control measures to counter museum and cultural centre threats:

Vibration sensors

- Placed behind exhibits or paintings
- Set off alarms with very light touch
- Can notify the control room of location for response

Exhibit inventory numbers

- Unique numbers to record each item on display and kept in a register
- Can be used to verify claims of found stolen items
- The register can keep detailed information about each exhibit that proves its genuine

Exhibit fixings

- Items such as paintings, sculptures and other movable exhibits can be bolted to walls or the floor to increase difficulty of theft

Glass casings

- Clear plastic or glass casing can be used to prevent touching of sensitive items
- The cases can be alarmed to alert if any tampering takes place

Environmental sensors

- Fire and smoke
- Temperature controls
- Humidity sensors

Viewing gaps

- Low rails around the perimeter of an exhibit
- Changes in flooring to signify 'no go' areas

Motion sensors

- Large areas of rooms can be covered
- Alarms sent to the control room with location
- Can cover areas not often used by visitors e.g.
    - Ventilation ducts
    - Delivery bays
    - Storage and maintenance areas

CCTV Cameras

- Used to monitor the site by security staff
- Record evidence and deter criminals
- Used to conduct surveillance of potential criminals at face identification level

20.4. Incident response options

Incidents may include fire, lost children, medical emergency and many other scenarios, however these incidents have been covered in previous sections of this book. For museums and cultural centres, the incident with the greatest risk is likely to be theft, and this will be covered in the next section.

20.4.1. Critical incident response

In the event of a critical incident, Security staff will follow established SOPs. A good guide for actions to take if an exhibit alarm is activated is to:

- If on duty in the alarm location, seal all entry and exit from the hall, zone or area.
- Control visitors and organise them into orderly groups
- Attempt to confirm if the alarm is legitimate or false
- Relay any information gained to the Control room
- Await the arrival of support from Security colleagues and police.

Museums and cultural centres require a unique knowledge of the environment, exhibits, significance to society and potential threats in order to effectively provide security, and Security staff will need to apply themselves to learning as much about the Museum or Cultural centre that they are working in.

Module 20 Revision

Revision questions

1. Define what an artefact is

2. List 4 major museums in the UAE

3. List 3 Security threats to exhibits in a Museum

4. List 4 Security measures available to secure exhibits within a museum

5. List the basic steps required of Security staff if a theft alarm is sounded

6. True or false? Security staff will be required to handle artefacts while on duty

TRUE / FALSE

7. List 3 potential environmental risks to exhibits at museums and cultural centres

Appendix A: lesson plans

Appendix B: Assessment

Appendix C: Presentations and materials