Operate basic security equipment

D1.HSS.CL4.03

Trainee Manual

Australian AID
asean
William Angliss Institute
Specialist centre for foods, tourism & hospitality

Operate basic security equipment

D1.HSS.CL4.03

Trainee Manual

Project Base

William Angliss Institute of TAFE
555 La Trobe Street
Melbourne 3000 Victoria
Telephone: (03) 9606 2111
Facsimile: (03) 9670 1330

Acknowledgements

Project Director: Wayne Crosbie
Chief Writer: Alan Hickman
Subject Writer: Alan Hickman
Project Manager/Editor: Alan Maguire
DTP/Production: Daniel Chee, Mai Vu

The Association of Southeast Asian Nations (ASEAN) was established on 8 August 1967. The Member States of the Association are Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand and Viet Nam.

The ASEAN Secretariat is based in Jakarta, Indonesia.

General Information on ASEAN appears online at the ASEAN Website: www.asean.org.

All text is produced by William Angliss Institute of TAFE for the ASEAN Project on “Toolbox Development for Front Office, Food and Beverage Services and Food Production Divisions”.

This publication is supported by Australian Aid through the ASEAN-Australia Development Cooperation Program Phase II (AADCP II).

Disclaimer

Every effort has been made to ensure that this publication is free from errors or omissions. However, you should conduct your own enquiries and seek professional advice before relying on any fact, statement or matter contained in this book. ASEAN Secretariat and William Angliss Institute of TAFE are not responsible for any injury, loss or damage as a result of material included or omitted from this course. Information in this module is current at the time of publication. Time of publication is indicated in the date stamp at the bottom of each page.

Some images appearing in this resource have been purchased from various stock photography suppliers and other third party copyright owners and as such are non-transferable and non-exclusive.

Additional images have been sourced from Flickr and are used under:

http://creativecommons.org/licenses/by/2.0/deed.en

http://www.sxc.hu/

File name: TM_Operate_basic_security_equipment_180413.docx

Table of contents

Introduction to trainee manual

To the Trainee

Congratulations on joining this course. This Trainee Manual is one part of a 'toolbox' which is a resource provided to trainees, trainers and assessors to help you become competent in various areas of your work.

The 'toolbox' consists of three elements:

- A Trainee Manual for you to read and study at home or in class
- A Trainer Guide with Power Point slides to help your Trainer explain the content of the training material and provide class activities to help with practice
- An Assessment Manual which provides your Assessor with oral and written questions and other assessment tasks to establish whether or not you have achieved competency.

The first thing you may notice is that this training program and the information you find in the Trainee Manual seems different to the textbooks you have used previously. This is because the method of instruction and examination is different. The method used is called Competency based training (CBT) and Competency based assessment (CBA). CBT and CBA is the training and assessment system chosen by ASEAN (Association of South-East Asian Nations) to train people to work in the tourism and hospitality industry throughout all the ASEAN member states.

What is the CBT and CBA system and why has it been adopted by ASEAN?

CBT is a way of training that concentrates on what a worker can do or is required to do at work. The aim is of the training is to enable trainees to perform tasks and duties at a standard expected by employers. CBT seeks to develop the skills, knowledge and attitudes (or recognise the ones the trainee already possesses) to achieve the required competency standard. ASEAN has adopted the CBT/CBA training system as it is able to produce the type of worker that industry is looking for and this therefore increases trainees chances of obtaining employment.

CBA involves collecting evidence and making a judgement of the extent to which a worker can perform his/her duties at the required competency standard. Where a trainee can already demonstrate a degree of competency, either due to prior training or work experience, a process of 'Recognition of Prior Learning' (RPL) is available to trainees to recognise this. Please speak to your trainer about RPL if you think this applies to you.

What is a competency standard?

Competency standards are descriptions of the skills and knowledge required to perform a task or activity at the level of a required standard.

242 competency standards for the tourism and hospitality industries throughout the ASEAN region have been developed to cover all the knowledge, skills and attitudes required to work in the following occupational areas:

- Housekeeping
- Food Production
- Food and Beverage Service

- Front Office
- Travel Agencies
- Tour Operations.

All of these competency standards are available for you to look at. In fact you will find a summary of each one at the beginning of each Trainee Manual under the heading 'Unit Descriptor'. The unit descriptor describes the content of the unit you will be studying in the Trainee Manual and provides a table of contents which are divided up into 'Elements' and 'Performance Criteria". An element is a description of one aspect of what has to be achieved in the workplace. The 'Performance Criteria' below each element details the level of performance that needs to be demonstrated to be declared competent.

There are other components of the competency standard:

- *Unit Title:* statement about what is to be done in the workplace
- *Unit Number:* unique number identifying the particular competency
- *Nominal hours:* number of classroom or practical hours usually needed to complete the competency. We call them 'nominal' hours because they can vary e.g. sometimes it will take an individual less time to complete a unit of competency because he/she has prior knowledge or work experience in that area.

The final heading you will see before you start reading the Trainee Manual is the 'Assessment Matrix'. Competency based assessment requires trainees to be assessed in at least 2 – 3 different ways, one of which must be practical. This section outlines three ways assessment can be carried out and includes work projects, written questions and oral questions. The matrix is designed to show you which performance criteria will be assessed and how they will be assessed. Your trainer and/or assessor may also use other assessment methods including 'Observation Checklist' and 'Third Party Statement'. An observation checklist is a way of recording how you perform at work and a third party statement is a statement by a supervisor or employer about the degree of competence they believe you have achieved. This can be based on observing your workplace performance, inspecting your work or gaining feedback from fellow workers.

Your trainer and/or assessor may use other methods to assess you such as:

- Journals
- Oral presentations
- Role plays
- Log books
- Group projects
- Practical demonstrations.

Remember your trainer is there to help you succeed and become competent. Please feel free to ask him or her for more explanation of what you have just read and of what is expected from you and best wishes for your future studies and future career in tourism and hospitality.

Unit descriptor

Operate basic security equipment

This unit deals with the skills and knowledge required to Operate basic security equipment in a range of settings within the hotel and travel industries workplace context.

Unit Code:

D1.HSS.CL4.03

Nominal Hours:

30

Element 1: Select and prepare security equipment for use

Performance Criteria

1.1 Identify and access security equipment to complete designated tasks in accordance with assignment instructions and organisational requirements

1.2 Perform pre-operational checks to equipment

1.3 Identify, rectify or replace faulty and damaged equipment

1.4 Identify and notify the need for training to the appropriate person

Element 2: Operate security equipment

Performance Criteria

2.1 Select, use and maintain appropriate personal protective equipment and clothing

2.2 Comply with all legislated and internal requirements

2.3 Operate security equipment in a safe and controlled manner

2.4 Monitor surveillance equipment

2.5 Test alarm sectors according to assignment instructions

Element 3: Maintain security equipment and resources

Performance Criteria

3.1 Return security equipment to operational condition

3.2 Clean, maintain and store security tools and equipment

3.3 Report faulty or damaged security equipment and items

3.4 Arrange back-up systems for faulty or damaged security equipment and items

3.5 Complete internal records and reports relating to security

Assessment matrix

Showing mapping of Performance Criteria against Work Projects, Written Questions and Oral Questions

		Work Projects	Written Questions	Oral Questions
Element 1: Select and prepare security equipment for use				
1.1	Identify and access security equipment to complete designated tasks in accordance with assignment instructions and organisational requirements	1.1	1 – 6	1
1.2	Perform pre-operational checks to equipment	1.1	7, 8	2
1.3	Identify, rectify or replace faulty and damaged equipment	1.2	9, 10, 11	3
1.4	Identify and notify the need for training to the appropriate person	1.3	12, 13	4
Element 2: Operate security equipment				
2.1	Operate security equipment	2.1	14, 15, 16	5
2.2	Comply with all legislated and internal requirements	2.2	17 – 20	6
2.3	Operate security equipment in a safe and controlled manner	2.2	21, 22, 23	7
2.4	Monitor surveillance equipment	2.2	24, 25	8
2.5	Test alarm sectors according to assignment instructions	2.2	26, 27	9
Element 3: Maintain security equipment and resources				
3.1	Return security equipment to operational condition	3.1	28, 29	10
3.2	Clean, maintain and store security tools and equipment	3.1	30, 31, 32	11
3.3	Report faulty or damaged security equipment and items	3.2	33, 34, 35	12
3.4	Arrange back-up systems for faulty or damaged security equipment and items	3.2	36	13
3.5	Complete internal records and reports relating to security	3.2	37	14

Glossary

Term	Explanation
Asp	Extendable/retractable baton
CAR	Corrective Action Report
CCTV	Closed Circuit Television
COP	Code of Practice
CPR mask	Disposable mask which must be used when performing cardio-pulmonary resuscitation
Contraband	Any item it is illegal to produce or posses
CO_2	Carbon dioxide – an inert gas used in some fire extinguishers
Comms	Communications/communication equipment
Discretionary power	Means staff have the ability to decide, on their own without referring to anyone else, what to do in the situation they are faced with: they have the 'discretion' to act one way, or another
Duty of Care	A legally imposed obligation on the venue and staff to take reasonable care to avoid causing foreseeable harm to guests. A staff member who is negligent in this regard breaches their Duty of Care and may be sued where injury or damage results
EAS	Electronic Article Surveillance
EDC	Everyday Carry (things carried on you all the time)
Emergency Management Plan	A document detailing the response of the venue/staff members when a variety of emergency situations arise
Evacuation	The safe & efficient removal of guests from a venue to a safe area in the event of an emergency
Fire blanket	A blanket made from fire retardant material, housed in a container (often near cooking equipment): when a fire occurs the blanket is withdrawn from the container, opened up & thrown over the pan/seat of the fire
ID	Identification; identity

Term	Explanation
IP	Internet protocol
LED	Light-emitting diode
OC spray	Oleoresin Capsicum spray (capsicum spray)
PA system	Public address system
PCI	Payment Card Industry
PPE	Personal protective equipment (and clothing)
QA	Quality Assurance
RFID	Radio Frequency Identification
SOP	Standard operating procedure
SOS	Generally understood signal to attract assistance/help: Save Our Sole
Sand bucket	A red-coloured bucket placed at strategic points around the venue containing sand to be thrown over a fire as a first response fire suppression method
Scope of authority	The extent to which you can make decisions and/or take action without reference to/asking permission from anyone else
Situational Awareness	Being fully aware of the environment you are in, and how, why and if it is changing
TIP	Threat Image Projection
UHF	Ultra-high frequency
U/S	Unserviceable
VDU	Visual Display Units
VHF	Very high frequency
VIP guest	VIP = Very Important Person. A VIP guest is an important guest (as defined by the establishment)

Element 1:
Select and prepare security equipment for use

1.1 Identify and access security equipment to complete designated tasks in accordance with assignment instructions and organisational requirements

Introduction

It is important to select the correct security equipment for the job to be completed.

This section identifies a range of security equipment, describes several security-related tasks which may need to be completed, provides an overview of assignment instructions and discusses organisational requirements which can apply.

Provision of security equipment

The security equipment used in venues:

- Will be provided by management
- Is often supplemented by personal property of security staff who frequently have preferences for carrying and/or using certain items.

For example, management may provide hinged handcuffs but individuals may prefer to use, and buy their own, chained handcuffs.

Security staff also often have strongly-held preferences for asps and torches/flashlights.

Management must always approve the use of any personal security equipment or items used by employees.

Variations in equipment

Security equipment used by staff may vary between venues.

Variations will occur based on:

- Layout of the venue – internally and externally
- Geographic location of the property
- Volume of trade, patronage or custom

- Hours the venue is open for business
- The proximity to other operations and the type/nature of those business and when they are open
- Type and nature of customers the venue attracts
- Previous history of the venue in terms of security incidents it has experienced
- Local and emerging trends in relation to security
- Number of staff employed
- Budget available
- Identified need regarding customer/guest expectations about security
- Personal items used/carried by individual staff.

Types of security equipment

Despite the potential for security equipment to vary between premises many common items (equipment and systems) exist:

Communication equipment

Communication equipment is required in relation to security:

- So management can communicate with security staff on an ongoing, day-to-day basis
- To communicate with security staff in the event of an emergency
- To allow security staff and management to communicate with each other
- So the venue can communicate with customers and guests
- To allow the venue to communicate with emergency authorities – such as when where there is a need to involve police, ambulance, fire or civil defence agencies).

Commonly used comms equipment includes:

- Hand-held two-way radios (UHF and VHF) – which may feature lapel microphones
- Communication headsets with earpieces – allowing the hands to be free for other work
- Landline telephones – such as the internal telephony system in a venue
- Cell phones – provided by management
- Pagers – of limited use but can be used as a back-up to summon assistance or ask a security officer to check in/contact someone

- Public address systems – can be used to communicate generally with customers, or the systems can be used in defined areas/sections (sectors) only
- Megaphones – for communicating with the public where the PA system does not operate, as an alternative to the PA system or during emergencies and evacuations.

Office equipment

Office equipment is needed to support the efforts of security staff by providing the standard services required by all departments/workers in a venue.

All venues with a security staff will have a dedicated office which will contain traditional equipment such as:

- Desks, chairs, cupboards, shelving
- Computers with internet connection – for general administrative tasks
- Printers – to produce hard copies of reports, plans, assignments
- Facsimile machines – to provide a back-up for email communication
- White boards – for planning and messages
- Photocopiers – for reproducing necessary documents
- TV monitor – for replaying surveillance vision
- Filing cabinets.

Personal protective equipment and clothing

A wide range of PPE and clothing is available for use by security staff.

These items will be identified in section 2.1.

Vehicles

Deepening on size, location and layout of the property there can be a need for security staff to use a variety of transportation options.

These include:

- Cars – usually:
  - Signed as ‘Security’ vehicles – but premises may use unmarked cars to enable covert surveillance, however most vehicles are intended to be a deterrent so high-profile/high visibility is important
  - Equipped with communication
  - Fitted with spotlight
  - Carrying flashing lights

- Vans – commonly used where there is a need to:
  - Carry guest valuable items
  - Provide escort to people
  - Move property assets
- Motorcycles – which:
  - Are more cost-effective than cars or vans
  - Can access areas cars/vans are unable to get into

- Bicycles – which:
  - Are extremely cost-effective
  - Enable the same quietness of a foot patrol while providing increased flexibility and coverage.

Fire fighting equipment

In-house training is essential before using ANY fire fighting equipment.

You must also make sure:

- You know how to differentiate between the different types of portable fire extinguishers – CO2, dry chemical, water: their different colours is the quickest way to tell them apart
- You know what extinguishers can be used on what types of fires – never use water extinguishers or hoses on oil, fat or electrical fires
- You know how to operate the extinguishers effectively
- You know where the fire hoses are and how to operate them
- You know where sand buckets are located
- You know where the fire blankets are and how to use them.

Fire fighting equipment can include:

- Water extinguishers – suitable for use on ordinary combustible materials but not safe for use on electrical fires or cooking oil/fat fires. They are ineffective on flammable and combustible liquid fires
- Foam extinguishers – dangerous if used on electrical fires. They are suitable for ordinary combustibles and for fires featuring flammable and combustible liquids
- Powder extinguishers – can be used on ordinary combustibles, fires featuring flammable and combustible liquids and electrical fires
- Carbon dioxide extinguishers are best for electrical fires – they have limited effectiveness on fires featuring flammable and combustible liquids, and cooking oil/fat fires
- Reels and hoses
- Fire blankets
- Sand buckets.

Fire alarms

Fire alarms are used to notify people within the establishment there is a fire.

Fire alarms may have different sequences (or tones) to indicate various levels of alert, such as:

- Stage 1 – indicates ‘There is a fire in the building but there is no need to evacuate’
- Stage 2 – indicates ‘There is a fire in the building and there may be a need to evacuate’
- Stage 3 – indicates ‘Evacuate now’.

Where such a system is in use you must know the sound of the different alarms and what they mean.

Always treat alarms seriously and regard them as genuine – never think 'it's only a drill', or 'it's probably a false alarm'.

Never turn a fire alarm off unless specifically ordered to do so by your supervisor.

Shut off valves

Depending on the type of emergency there may be a need to turn off supply valves.

In the event of a fire (for example) you may be required to:

- Turn off the electricity – at a meter box or similar
- Turn off the gas – using a shut off valve.

In the event of other emergencies you may also be required to shut off the water (using a gate valve or similar).

Intruder alarms

These can give an audible or visual warning (or both) that unauthorised access has occurred in an area.

May be activated by a pressure pad, beam, motion sensor or when a contact is made or broken.

All alerts generated by these alarms must be investigated.

First aid kits

Most venues will ensure at least one person with current first aid training is rostered on duty at all times.

The venue will also usually provide:

- A comprehensive first aid kit in a central location – such as Head of Security office or manager's office
- Smaller first aid kits – in security vehicles and nominated other areas (perhaps at front office, in the housekeeping department or behind bars.

In addition some larger venues will also have a dedicated first aid room and may have their own doctor, or nurse.

These properties will have a much larger range of first aid equipment which can include:

- Oxygen
- A defibrillator.

Torches or flashlights

Flashlights are standard equipment and are used not only at nights but also to illuminate dark areas during daylight hours.

You must know:

- Where torches are located
- How to operate them
- How long they will last.

Most security staff will use nothing but a Maglite® with many preferring the standard 4-cell (or 5-cell or 6-cell) LED version (which can be used as a weapon), while many others opt for the more compact LED versions (such as the MagTac®) which is lighter and easier to carry/put on a duty belt.

The flashlight you use should:

- Be powerful
- Contain a strobe facility – which can be used to attract attention or signal your location as an SOS function.

Signage and barriers

Important security-related items also include:

- Warning signs
- 'Do Not Cross' and 'Do Not Enter' tape
- Witches hats.

Camera

Some venues provide security staff with cameras.

A compact movie camera can be part of your EDC and used to:

- Capture evidence – for referral to the authorities; to support an insurance claim; to provide the basis for civil action against offenders
- Deter threats – many people will withdraw if they believe they are being filmed
- Record details/occurrences during an event/incident – which can be used later for analysis, identification and examination/investigation.

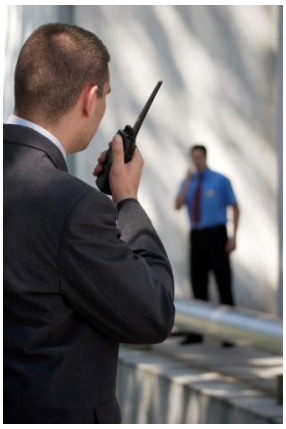
Designated tasks

The tasks security personnel are required to undertake include:

- Conducting routine security monitoring of the premises – these can include:
  - Regular foot and vehicle patrols
  - Static guard duties – providing a visible presence at an entrance or designated location

- Performing crowd control duties – which can include:
  - Directing people
  - Controlling vehicle movement – which can include controlling parking and traffic speed
  - Preventing access to certain areas
  - Deterring and responding to unacceptable behaviour
  - Assisting patrons as required
- Undertaking screening activities – of people and/or property, which may involve:
  - Operating luggage X-ray machine
  - Policing electronic doorways/frames
  - Using hand-held wands
  - Inspecting and checking vehicles

- Checking identification of customers – with reference to:
  - Ensuring under-age people to not enter licensed areas
  - Only authorised persons are on the premises
- Escorting people – to:
  - Protect individuals or groups
  - Safeguard their property
  - Deliver required services to VIP guests or those who request it



- Controlling access to the venue or designated areas – to:
  - Deter unwanted people
  - Assist guests and customers
  - Refuse access to those who are unwanted or not entitled to be on the premises
  - Check age and ID of people
- Monitoring egress of persons from the property – to:
  - Control noise
  - Prevent theft of assets
  - Assist as required
  - Respond to unacceptable behaviour
- Responding to alarms – this is a central role of security staff.

  All alarms must be responded to and investigated.

  It is CRITICAL you never believe an alarm is a false alarm even though the past 100 alarms have been.

  Thieves often trigger regular false alarms in a certain area to lull staff into thinking the *next* alarm will also be a false alarm and therefore not worthy of a response – you must respond to all alarms, every time without exception.

- Working with security-related documents – such as:
  - Creating patrol schedules and routes
  - Developing plans for special escorts and carry requirements
  - Making revisions to existing plans and SOPs
  - Generating reports
  - Completing checklists.

Assignment instructions

'Assignment instructions' are instructions provided by management to staff about activities they are required to undertake.

Some assignment instructions will be in writing but the majority will simply be verbal instructions.

Situations commonly requiring written instructions

Written assignment instructions are common for situations such as:

- Special surveillance of an area of person
- Investigation into an event or incident
- Escort duties
- Special or substantiated threats from multiple targets or previous offenders
- Responses based on advice from external authorities
- Responses to situations where risk assessment has determined there is a high probability and a substantial potential (negative) result/outcome

- Large events (which may be defined by numbers attending, variety of activities, range of venues being used) where specialist security action is required (such as crowd control, security checks, vehicle inspections, traffic control, liaison with authorities).

Details traditionally included in assignment instructions

Regardless of whether assignment instructions are given verbally or in writing they will/should address the following:

- Any specific requirements identified by a guest – in relation to the provision of service, such as:
  - Number of staff required
  - Skills and or experience required
  - Meeting points
  - Timing issues
  - Known or anticipated threats
  - Threat levels

- Objectives for the assignment – which may be:
  - Patrol
  - Escort
  - Monitor
  - Surveillance
  - Investigation
- Special access arrangements – as appropriate to the circumstances, including reporting requirements 'on arrival'
- Time on and time off – duration of assignment
- Specific work tasks which comprise the assignment – for example an assignment may be 'Provide security for guests arriving at ASEAN symposium' and the specific work tasks may be:
  - Monitor vehicles on arrival and restrict vehicular access to central car park only
  - Oversee unloading of vehicles
  - Scan luggage of all arrivals into Ballroom
  - Check ID of all attendees
  - Patrol toilets, entrance foyer and Asian Room

- Integration of assignment-specific duties with other normal/scheduled security obligations and tasks
- Resources to be used to achieve the objectives – these can include requirements relating to:
  - Human resources – by name and number
  - Physical resources – such as barricades, scanning devices, comms, PPE, weapons
  - Intelligence – information about the event/situation
- Management – detailing:
  - Who is in charge
  - Reporting protocols
  - Command and control authority

- Documentation – involving:
  - Issuing of relevant forms, logs, registers as appropriate to/necessary for the assignment
  - Provision of relevant plans, routes and schedules
  - Distribution of any paperwork needing to be completed as part of the assignment, or when the assignment has been finalised.

Online information

Equipment and items

- http://www.alibaba.com/showroom/hotel-security-equipment.html
- http://www.motorola.com
- http://www.systemteq.com/hotel-security.htm
- http://weien.en.alibaba.com/product/370593456-200123753/hotel_security_equipment_GC_1001.html
- http://www.digisec.com/resort_facilities.html
- http://www.alibaba.com/showroom/hotel-security-equipment.html
- http://w3.siemens.com/market-specific/global/en/hospitality/hotels-resorts-casinos/hotel-safety-security/hotel-security/pages/hotel-security.aspx.

Using fire extinguishers

- http://www.youtube.com/watch?v=ZCSms-jyOao
- http://www.youtube.com/watch?v=0wahXwItLRY.

1.2 Perform pre-operational checks to equipment

Introduction

All security equipment must be checked before it is used.

This section stresses the need for these checks and describes what is involved.

Importance of checks

Security equipment must be checked:

- Before it is used – on every occasion without exception
- By every staff member taking equipment for use – regardless of who they are.

These checks are important because:

- Every item must work as expected when called on to do so
- You must ensure the safety of the item before you take it/use it
- The life you save may be your own
- Guests and management expect you to be equipped with equipment which worked/functions when needed
- Not ensuring you have fully-operational equipment may be interpreted as a breach of your Duty of Care obligations.

Never assume an item is fit to use simply because:

- Someone else just handed it in at the end of their shift
- Nothing has been documented about it

- It is or it looks new
- It has never been a problem in the past.

There is nothing worse – or potentially more dangerous (even fatal) – than reaching for an item of equipment only to find it does not work as expected.

Pre-operational checks

There are a wide variety of activities comprising pre-operational checks and most people would not appreciate what is involved.

Standard activities include:

- Checking log books and maintenance registers – to see if items have been logged as presenting problem/operational issues recently. Where there are multiple items of the same type (such as torches, handcuffs, batons or pepper/OC spray) they will each have their own individual identifier/ or number to distinguish one item from another
- Reading/referring to manufacturer's instructions – where you are not familiar with all the aspects of an item (such as a conveyor X-ray machine) you will need to read these instructions in order to:
  - Identify the checks or tests which need to be undertaken
  - Determine how to conduct the tests or checks
  - Verify the results/outcomes of the tests or checks

- Using your senses to determine operational readiness – this can involve:
  - Visual observation of the item
  - Verifying lights have illuminated as required
  - Listening for sounds/noises which indicate a problem – including audible alerts (from system checks)
  - Conducting alarm tests – for fire boards and intruder alarms
- Responding to small operational defects by, as appropriate:
  - Cleaning items
  - Priming
  - Tightening – connections, nuts, screws
  - Undertaking basic repairs – according to User Manuals/Operating Instructions

  - Making adjustments – to (for example) clearances and tension, location and line of sight, focus, settings and sensitivity
- Undertaking basic preventative vehicle maintenance (a checklist may be provided to assist) – such as:
  - Checking oil
  - Checking water

  - Filling with fuel
  - Verifying tire pressures
- Undertaking basic vehicle-related checks (a checklist may be provided to assist) – such as:
  - Testing comms/radio
  - Testing spotlight
  - Verifying first aid kit
  - Testing headlights and flashing lights
  - Verifying presence of other standard in-car assets

- Other testing and checking – such as:
  - Running diagnostics on nominated systems – which will self-diagnose issues
  - Making test transmissions on two-way radio
  - Weapons:
    - Are loaded – spare ammunition is available as permitted
    - Mechanisms works
  - Verifying charge on cell phone
  - Verifying charge on rechargeable torch
  - Shaking sprays to determine if contents are sufficient for shift/upcoming assignment.

1.3 Identify, rectify or replace faulty and damaged equipment

Introduction

If an item is identified as being faulty or damaged during a pre-operational check it must be rectified or replaced.

This section addresses activities involved in this process.

Identifying faulty or damaged equipment

Faulty or damaged equipment may be identified:

- As a result of pre-operational checks
- When reported to you by other staff
- When flagged by the system as needing attention.

Examples of faulty or damaged equipment

There is a very liberal interpretation of what constitutes ‘faulty or damaged equipment’.

Items do not need to be ‘broken’ to require attention.

Examples of faulty and damaged equipment can include

- Missing items – these can be:
  - Items which have been removed for repair or service – that is, they may have been returned to the manufacturer or supplier for service or they may be with the Maintenance department being repaired
  - Items which have been stolen or misplaced – it is relatively common for smaller security item to 'go missing' when an event occurs
  - Items which have been disposed of – because of their condition or age
- Items which have flat batteries – or batteries which will no longer hold an effective charge for the required period
- Torches with blown globes
- Items (equipment, machines and systems) requiring:
  - Preventative maintenance in accordance with established servicing schedules
  - Service in response to requests for repairs/maintenance
- Any item which works intermittently
- Any item which it dangerous to use – for whatever reason (dangerous to you or members of the public)
- Any item or system which fails to operate as intended.

Note: many systems, pieces of equipment and items will present with one aspect not performing as intended but all other features showing full operational readiness.

In these cases items are usually kept in service if the one aspect is a relatively minor component of the overall system/item.

Action to take where a problem is identified

When you identify an issue with equipment you must follow house procedures.

There will usually be SOPs for:

- Items which can be fixed
- Items which cannot be fixed.

Items which can be fixed

Your on-the-job training will:

- Explain your scope of authority for repairing security equipment – detailing:
  - The items you can attempt to repair/fix – for example:
  - Replacing batteries and globes would be approved
  - Adjusting trigger pressure on a firearm would not
  - Oiling the lock on handcuffs would be authorized
  - Attempting repairs to a conveyor belt on a scanner which is under warranty would not

- Adjusting the sensitivity of a walk-through metal detector would be approved
- Re-aligning CCTV cameras to cover different areas would not
- Limits regarding aspects such as:
- Time to be spent on fixing the problem
- Budget
- Where repairs can be undertaken
- When/if you are authorized to call in an external service provider to undertake immediate on-the-spot repairs in (say) an after-hours situation

- Provide instruction on how to:
  - Trouble-shoot – diagnose and determine causes of faults
  - Repair, service and maintain items you have been authorized to work on.

Additional points to note

- You must never assume you know what is wrong with an item unless you have been properly trained in diagnosing faults
- You must adhere strictly to your delegated scope of authority – failing to do so can have legal implications where the repair causes a problem or breaches the legally-binding requirements of a service contract, guarantee or warranty
- Just because you know how to repair one type, brand or model of equipment does not mean you can automatically repair all similar (but different) types, brands and models
- You must never ignore a fault or problem – you must either:
  - Fix the issue
  - Make arrangements for required repairs/service
  - Report the issue.

Items which you cannot fix on-the-spot

All venues will have some standard/formalised procedure for addressing these situations which will usually entail:

- Identifying and tagging the item – as 'U/S'
- Segregating the item from other items – so others do not take/use it and they know it is unavailable
- Taking action to initiate repair or replacement – such as:
  - Completing a 'Maintenance Request form'
  - Handing the item in to a designated person/department
- Attempting to arrange a replacement or substitute item
- Reporting the situation problem – which may require:
  - Verbal notification
  - Some form of written form/report
- Calling in an external technician (where authorised under your scope of authority) so immediate on-site service/repair can take place.

1.4 Identify and notify the need for training to the appropriate person

Introduction

There is an ongoing need to be alert to the need for security training.

This section discusses who such a need may apply to, what it may relate to and who such need may need to be communicated to.

Those who may need training

Traditionally security training may be required by full-time, part-time and casual staff as follows:

- New employees – people who are new to the industry and new to the venue
- Existing employees who have transferred to duties involving security work/responsibilities
- Experienced staff – who have worked in security at other venues but not at their current workplace
- Contracted security staff from an external security company who have no previous experience at the venue – these people may be used:
  - To support when a large event is taking place
  - To support when a specific threat has been identified
  - To replace a staff member at the last minute who has:
    - Not attended for their rostered shift
    - Had to leave work due to accident, injury or illness.

Issues training needs may relate to

Given all new staff will require the basic security training deemed necessary by their employer, other security-related training needs arise when:

- New equipment is bought and/or installed
- Breaches of security occur
- Established protocols prove ineffective in addressing a situation
- Employer introduces new (or revised) policies and procedures – nearly all new/revised policies and procedures have the potential to impact existing security arrangements or protocols
- A new target market/demographic is attending the venue
- The property changes its opening/trading times
- New attractions are brought into the venue which alter demand/patronage

- Legal action has been taken against an employee or the venue
- Adverse media attention occurs about the conduct/operation of the venue
- Authorities advise the venue needs to improve/modify its security
- Authorities warn the venue of an identified/expected new threat
- The layout of the property changes – which creates new risks, choke points/bottlenecks and potential for theft and other issues
- A special or important event is expected
- A VIP guest requires special security arrangements not normally provided by the venue.

Reporting to the appropriate person

When the need for security-related training has been identified the normal course of action is to put the identified need into a formal written request and submit it to the 'appropriate person' or group in the venue.

This may be:

- Owner
- Manager
- Head office
- External security provider – where the venue out-sources its security
- Head of Security
- Venue trainer
- Department supervisor
- Safety and Welfare (or similar) Committee
- Equipment manufacturers – suppliers of systems and large equipment will often provide training on their items (sometimes free; sometimes on a fee-for-service basis).

Report contents

The report must detail:

- Number of staff requiring training
- Names of staff – with contact details
- Urgency of the request for training
- Specification of the type/nature of the training required.

Work Projects

It is a requirement of this Unit you complete Work Projects as advised by your Trainer. You must submit documentation, suitable evidence or other relevant proof of completion of the project to your Trainer by the agreed date.

1.1 Interview a Security Officer (or other appropriate person) from a venue and prepare a written submission which details the following:

- Security items and equipment used at the venue
- What those items are used for
- Pre-operational checks made on each item.

1.2. Name one item of security equipment identified in your answer to Work Project 1.1 and contact a venue, a security company/provider or the manufacturer and prepare a report which:

- Lists common faults/problems with the item
- Explains how to identify the faults/problems
- Describes action that can be taken to rectify those faults/problems.

1.3. Contact a local venue and/or local authorities and identify mandatory training required for those who wish to work as a Security Officer.

Summary

Select and prepare security equipment for use

When selecting and preparing security equipment for use:

- Use equipment and items provided by management
- Supplement venue items with your own personal gear (where permitted)
- Make sure you know all the security gear available from and used within the venue
- Learn the tasks and responsibilities security is expected to discharge
- Match tools and equipment to work to be done
- Determine house policies and protocols as they apply to security work and use of security items
- Become familiar with workplace assignment instructions
- Check equipment, tools, items and systems prior to use
- Make sure all faults and damage are rectified or reported
- Be alert to the need for training to address use of new equipment and/or emerging security situations and threats.

Element 2:
Operate security equipment

2.1 Select, use and maintain appropriate personal protective equipment and clothing

Introduction

This section presents a range of personal protective equipment and clothing used or worn by security personnel and discusses factors related to its selection, use and maintenance.

Background to PPE

PPE defined

PPE:

- Stands for Personal Protective Equipment
- Includes reference to protective clothing.

Who provides PPE?

PPE is usually supplied by the employer.

Certainly the employer will provide a uniform with basic PPE.

Individuals may elect (subject to permission from management) to enhance the issued PPE with additional items: these items are provided, paid for and maintained by individual staff.

Where the employer provides PPE, its use is mandatory: it is not optional as to whether you wear/use the items or not.

All items provided by the employer are maintained by the employer.

PPE and its uses

The following is an indicative list of items and their uses:

Body armour

These are items worn to protect the body against bullets and knives.

They can be covert (worn so they cannot be seen – so it does not alarm guests) or overt (meaning they are worn 'obviously') sending a message to potential aggressors you are aware of a threat and are prepared for it.

Body armour is not commonly worn and most venues will not have body armour as part of their standard stock of PPE.

Protective shields

Protective shields provide personal protection in close contact/crowd control situations and may be used as equipment to encourage/force people to 'move away'.

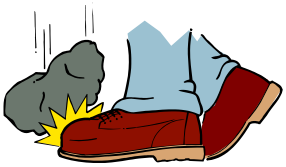
Masks

Masks are used to protect the face and eyes against:

- Physical attack
- Gas attack.

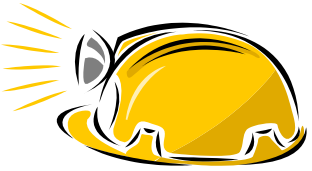
As with external/overt body armour, wearing a mask signals preparedness and readiness to act.

Safety boots



It is a standard requirement all security staff wear steel-capped boots for personal protection of the feet as well as enabling a supplementary attack option.

Head protection



Helmets are not commonplace in venue security as they tend to alarm guests.

Where planning and analysis of a situation indicates helmets are required they will usually need to be borrowed, bought or hired.

Once again, wearing a helmet conveys an image of readiness, willingness and preparedness.

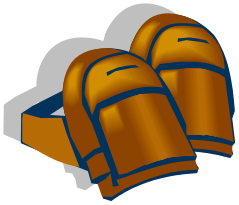
Safety glasses

These are commonly combined into head gear or masks and are used when personal attack is expected to protect the eyes.

They should protect against acid attack.

Again, wearing safety glasses can be part of the intimidation provided by a fully-equipped officer in an incident response situation.

Knee pads



May be worn in crowd control situations to protect the knees in the event you are pushed to the ground.

As with steel-capped boots, they also provide an attack option.

Duty belt

Also known as utility belt this is used to carry equipment/items you require when undertaking security work/patrolling the premises.

You may be supplied with this belt by the venue or you may purchase your own.

The duty belt has **many** attachments and holsters/pouches which carry the equipment.

It is your choice as to how your belt is set up (that is, exactly where on the belt you position items).

A standard belt set-up for staff who are not armed should include:

- Pager holder – with pager
- Flashlight holder – with torch
- Asp/baton holder – with asp or baton
- Handcuff pouch – with handcuffs
- Comms holster – for radio
- Medical pouch – containing disposable gloves and CPR mask
- OC spray carrier – with spray
- Key holder – with handcuff keys and other keys as required
- Camera case/pouch – with camera
- Knife holder – with knife.

A duty belt for an armed officer will add a pistol and holster plus one (or two) magazine pouch to house an extra clip of ammunition.

The duty belt is attached to your normal belt by a number (six to eight) of belt-keepers. The duty belt does not replace the belt you use in your trousers.

A word about neck ties

Many/most uniforms for security staff do not require the wearing of neck ties.

Where they are required they should always be of the clip-on type so they pull off if someone grabs them.

This prevents an aggressor being able to pull you towards them when they grab your tie.

Maintenance for PPE

The generic requirements for maintaining PPE are:

- Inspect after reach use
- Clean after each use
- Replace or repair when damaged – the preference is for replacement
- Follow manufacturer's instructions
- For battery-powered items:
  - Re-charge as required
  - Fit with new batteries as required
- Return items to designated storage locations after maintenance/cleaning – so they are available for others to use.

2.2 Comply with all legislated and internal requirements

Introduction

All security staff must comply with all relevant legislated and internal requirements.

This section discusses compliance obligations for security staff.

Basic roles

It is vital security staff understand the legal limitations relating to what they are entitled to do when working as security staff.

In the main, **security staff can do little more than other staff or members of the public** when it comes to responding to incidents and when taking action in response to unacceptable behaviour by people.

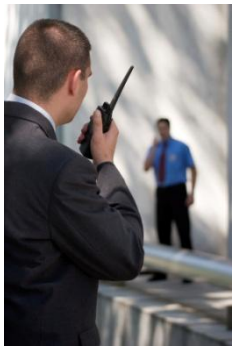
Security staff do not have 'a right' to:

- Bully
- Harass
- Intimidate
- Assault.

Deter, detect, defend and detain

In essence the four main roles of Security staff are to:

- Deter:
  - Guests from behaving in an unacceptable manner – by their physical presence
  - Theft from the venue – through their loss prevention activities (observing activities and people (staff and patrons), monitoring alarms and anti-theft devices (including EAS devices), patrolling areas
- Detect:
  - Offences which have been committed
  - Unauthorized access to, and use of, facilities
  - The presence of people on the premises whose presence renders the venue liable to an offence – such as identifying intoxicated persons or under-age people on the premises



- Defend:
  - People from unwanted and/or potentially dangerous/harmful or offensive actions or behaviour of others
  - The property against damage
- Detain:
  - People who have broken the law – see 'Making an arrest' (below).

The role of service provision

Security staff in hospitality venues must realise they are working in a 'service industry' meaning:

- An important part of their job is to provide service to customers/guests – owners and managers expect security staff to do this and so do customers/guests
- The attitude and disposition of security staff needs to be one of helpfulness and service rather than one of intimidation and harassment.

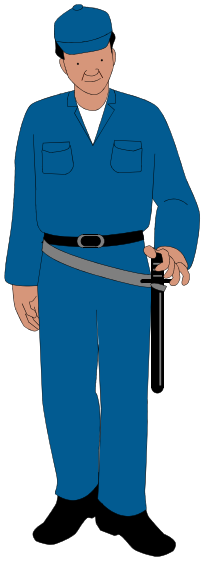
Legal compliance obligations

In order to work as a security person the following requirements generally apply but you need to check what applies in your country and in the specific venue where you are employed.

You **may** need to:

- Undertake and successfully complete nominated security training/courses – in some countries/regions/locations there can also be a need to undertake refresher training every two to three years to maintain currency of accreditation/certification
- Provide your employer with proof of:
  - Training which has been completed
  - Currency of certification
- Wear nominated identification so members of the public can:
  - Identify you as a member of security staff
  - Identify you as a specific individual by name or number

- Adhere to the requirements of national or local guidelines developed to govern the actions of security staff in order:
  - Members of the public can have faith and confidence in them
  - Their actions are controlled so they remain legal and ethical



In addition you **will** need to:

- Complete necessary official training if you wish to carry a firearm
- Complete any internal, on-the-job training required to familiarize you with venue requirements, SOPs, systems, venue layout and the unique factors relating to individual properties or tasks
- Adhere to the standards and protocols of your employer when undertaking security work
- Meet all relevant QA standards as they apply to the security work being performed
- Comply with the laws of the country as they apply to security work and the limitations and restrictions imposed on anyone undertaking security work
- Be responsible for your actions – every action you take (or elect not to take) is always subject to scrutiny and analysis: always remember you are on show to the public and someone (or something) is *always* watching you.

You are not a police officer

It is extremely important you understand **performing security work in a venue does not make you a police officer**.

You do not have the same rights as a police officer.

You do not have the same right to stop people or to *demand* their name. You may, of course, request it/ask for it but people do not have to comply.

As already stated your rights as a security officer are, in reality, no more than the rights of the ordinary citizen.

Your 'power'/'authority' often comes from:

- The fact you are in uniform – and most people respect the uniform
- Your demeanour/attitude and appearance – and sometimes your size.

The reality of many security jobs is if a problem occurs your job is to:

- Contain the situation to the best of your ability – by, for example:
  - Moving people away from the situation
  - Restricting access to an area
- Call for assistance from external security or local authorities
- Protect and defend – always put the protection of lives/people above the protection of assets/physical resources (including cash).

Making an arrest

The brief advice is – Don't!

Making a citizen's arrest may look and sound fine on the television, but that is not the reality of most situations.

There is too much that can go wrong – from physical violence and assault through to possible legal action for wrongful arrest/detaining a person against their will (or similar).

If an arrest is required or there is a need to detain a person you must be very careful you can:

The best advice is to 'delay' the person (the alleged offender) from leaving until the police arrive and then letting them deal with the situation.

Discuss this with your venue and be guided by them and specific house policy.

Strategies to delay 'offenders' until police arrive can include:

- Engaging the person in conversation
- Asking them questions
- Providing them with a drink or something to eat
- Asking them to wait for the police to arrive.

2.3 Operate security equipment in a safe and controlled manner

Introduction

Security equipment must be operated in a safe and controlled manner at all times.

This section discusses requirements in this regard.

Following manufacturer's instructions

Basic requirements

The Golden Rule is all security items must be operated in accordance with whatever manufacturer's instructions apply.

Even basic items of equipment such as flashlights and handcuffs come with User Instructions so you must:

- Obtain these
- Read them
- Implement what is required.

User Instructions are also extremely useful when trying to diagnose a fault/problem as they normally include a Troubleshooting Guide.

Manufacturer's instructions will relate to equipment and systems/technology.

Equipment

Examples of instructions which will relate to equipment can be expected to address:

- Information about the construction and performance rating of items
- Identification of situations in which the item is suitable for use, and not suitable for use –mentioning as appropriate to the item:
  - Limitations
  - Breaking points
  - Distances/coverage
  - Power
- Directions relating to:
  - Preparing the item for use – standard/daily checks; regular/periodic checks
  - How to use the item – which can be expected to address (depending on the item):
    - How to hold them
    - What buttons and switches are for
    - Safe-in the item (that is, carrying it so it is safe and will not accidentally or inadvertently deploy)
  - Preventative maintenance and servicing
  - Troubleshooting and repairs.

Systems and technology

'Operating Instructions' or a 'User Manual' will usually accompany any security systems or technology you are expected to operate.

In addition there will normally also be:

- On-the-job training provided by the suppliers of the equipment/technology
- Supplementary internal training provided by your employer.

Examples of instructions will of course vary between the type and version of systems and technology being used.

Operational instructions you will need to learn can be expected to address:

- How to turn the system/technology on and off:
  - To log on and log off
  - To access nominated sections of the system
  - To access/read nominated sectors of the business

- How to run system checks – where the system/technology conducts internal audits of its capacity and generates a Situation Report' detailing the 'status' of all its component parts
- How to adjust element of the system – such as:
  - How to focus cameras
  - How to adjust sensitivity of scanners
  - How to change passwords and access codes

- How to access parts of the system:
  - To run checks
  - To retrieve data
  - To interrogate the system
  - To generate hard and soft reports
- How to enter data into the system:
  - To update information and data fields
  - To add new staff – or remove access for nominated staff
  - To accommodate SOPs for data entry, archiving data and completion of records, reports and electronic documentation

- How to operate and read alarms systems – including:
  - Determining type and location of threat or problem from an alarm board, indicator or other system alert
  - Knowing how to activate and de-activate the entire system or required aspects of it.

Following internal requirements

You will become aware of internal requirements regarding operation/use of security equipment:

- Through discussions with your colleagues and supervisor
- By observing their actions
- As a result of formal, internal training.

There is a high-level consistency throughout the industry as to the internal requirements security staff are expected to comply with when performing their duties:

- Exercise personal control at all times – customers can be very abusive and even antagonistic but it is important you control your response and never resort to verbal or physical abuse
- Use tact and diplomacy at all times when interacting with members of the public
- Focus on the use of appropriate communication and interpersonal skills (such as discussion, mediation, conflict resolution, negotiation) rather than physical alternatives or the use of force
- Communicate in a polite and respectful manner using moderate language and avoiding offensive language and swearing
- Act fairly towards all guests and members of the public – do not discriminate on the basis of (for example) age, gender, race or religion)
- Use restraint when a physical response is necessary – you never have the right to use more than 'reasonable' force to address a situation/threat
- Refrain from searching people
- Only use security items for their intended purpose
- Observe the requirements of the venue Privacy and Confidentiality policies at all times
- Never discuss revenue, occupancy levels or matters to do with security, cash movement, asset protection protocols (guards,. patrols, routes, alarms, position of cameras, response plans/options) with anyone
- Do not discuss security-related matters or responses to incidents/threats with the media.

User Instructions

See the following online information:

- http://www.wi-ltd.com/security/Scanning_and_Screening/X_Ray_and_Screening_Systems/Baggage_Scanners/WG_IS6545_X-Ray_Hand_Baggage_Scanner
- http://www.protectwest.com.au/manuals/Ademco%20Vista%2050%20user%20manual.pdf
- http://www.adtsecurity.com.au/home-security/resource-centre/alarm-panel-user-manuals.

2.4 Monitor surveillance equipment

Introduction

Conducting patrols and monitoring surveillance equipment are usually the two primary duties of security staff.

This section discusses the common, generic activities involved in monitoring surveillance equipment.

Unique nature of surveillance equipment

Surveillance equipment (systems and technology) will vary between venues.

There is also no precise definition of exactly what 'monitoring' is or what 'surveillance equipment is.

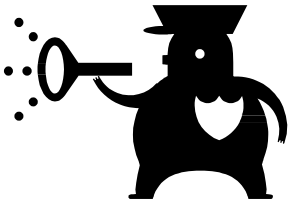
Monitoring defined

These notes define monitoring of surveillance equipment as:

> *"A combination of observations relevant to the security systems and technology deployed in the workplace."*

Monitoring activities

Practical workplace need, coupled with the above definition means monitoring activities will include:



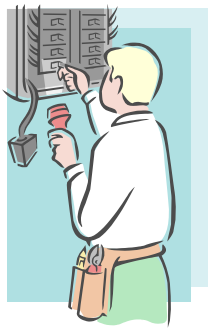
- Using your basic senses – for example:
  - Watching for visual alarms – flashing lights, illuminated displays
  - Listening for audible alarms – bells, sirens, tones
  - Being alert to environmental cues – such as open doors which should be closed, unlocked doors which should be locked, unattended items, suspicious persons, loud noises/shouting, indicators of distress, unacceptable behaviour
  - Noticing smells – which may indicate smoke/fire, a gas leak, a chemical spill, a petrol leak

- Watching alarm and security boards and monitors/screens to:
  - Immediately identify activation
  - Locate site of alarm
  - Notify internal personnel and external authorities – in accordance with alarm type and SOPs
  - For example, many venues require **immediate notification** of fire authorities when a fire/smoke alarms activates even before the alarm is investigated and/or even though flames cannot be seen and there is no smell of smoke
  - Where this SOP applies it is a mandatory requirement *regardless* of when the alarm is detected or where the fire/smoke has been detected

- Following all manufacturer's instructions for the use of all aspects of the security technology in use – this may apply to:
  - Setting up equipment in accordance with manufacturer's instructions – for items such as:
    - Sensors and detectors
    - Screens, monitors and boards
    - CCTV cameras – with special attention to line-of-sight/coverage, and picture resolution
    - Walk-through and conveyor-belt scanners

  - Conducting system checks – which relates to:
    - Scheduling and implementing regular system checks – to check for correct operation of the system and alerts/alarms
    - Running system diagnostic checks
    - Cleaning component parts
    - Verifying actual coverage by the system is in accordance with expected/required coverage
    - 'Green lights and red lights' – referring to visual monitoring of system displays which indicate (as appropriate to different systems):
      - Normal operation – 'nothing detected'
      - Issues and alerts – to be investigated
    - Testing – such as verifying alarms are operational, surveillance cameras can be remotely controlled, test packages are run through X-ray machines and scanners

- Completing necessary logs, forms and registers – these have to be completed to provide evidence of actions such as:
  - **All activities** identified/described immediately above
  - Responses to system alerts and alarms
  - Corrective action taken to address identified problems with systems/technology.- a CAR may need to be completed
  - It is vital you understand it is never sufficient just to respond to a situation, you also have to record your response as evidence of your action



- Checking and assessing system data and records – to verify:
  - Required information is being captured
  - Reliability of system for capturing the data
  - Accuracy of data being recorded
- Checking internal signage – where there is a legislated requirement the venue informs patrons electronic surveillance is being used on the premises, part of the monitoring must be to ensure the required signs are displayed in the required areas and are clearly visible ('This venue is under contact video surveillance')

- Checking the coverage by CCTV cameras does not breach the privacy rights of citizens – basically this means ensuring the CCTV cameras do not film public areas which are not part of the venue
- Verifying the surveillance records are being maintained for the required period of time – such as proving to yourself (and recording this fact) all surveillance tapes/discs are on file for (usually 14 days) and are dated in such a way to aid easy retrieval of footage as required.

TIP

Some makes and models of baggage scanners (conveyor belt, X-ray type) will insert a Threat Image Projection into items being scanned to test the observation/detection skills of the operator and/or to determine if they are paying attention to the display/items being scanned.

For example, the system will show a suspicious item as being detected in the luggage (such as a gun or knife).

If the operator notices and queries this image the system will respond by identifying the image as a TIP indication no action is required.

If the operator does not detect the item the software will record this operator error so management can identify whether the operator requires training, or should be replaced by someone else.

Situational Awareness

The combination of the above should produce a situation where you are fully aware of everything happening in your environment: this is referred to as 'Situational awareness'.

Situational awareness may be seen as being completely aware of the environment/situation you are in and knowing if it is changing, how it is changing, and why it is changing.

Situational awareness relies heavily on:

- Keeping your eyes and ears open – to keep the inflow of information coming in to you/your senses
- Analysing everything:
  - What was that noise?
  - Why did the noise happen?
  - Where did it come from?
  - What does it indicate?
  - What action do I need to take in response?

Situational awareness is the basis for:

- Determining threat situations
- Identifying action needing to be taken
- Identifying what is 'normal' and things are not normal
- Prompt and effective responses.

2.5 Test alarm sectors according to assignment instructions

Introduction

For alarm systems to be effective you must know they are operating as intended.

This section looks at system testing introducing the concept of testing alarm sectors.

Need to test all alarms

Alarms must be regularly tested to ensure they are operating as intended.

Undertaking these tests is part of 'responsible management' and duty of care obligations.

To be effective, all systems must be tested.

This means testing needs to be undertaken on all systems to which alarms are attached – this means testing can extend beyond the traditional 'security' systems into other systems which monitor building performance.

Sometimes testing is performed by the Maintenance department, sometimes by external consultants/service providers and sometimes all systems testing is integrated into the work of security staff.

Systems which may need to be checked include:

- Fire alarms
- Smoke and heat detectors
- Intruder alarms – including local alarms on fire doors/exits which are triggered when the door is opened
- Alarm boards and VDUs
- CCTV – including checks on:
  - Infrared security cameras (so-called 'night vision' cameras)
  - Dome ('eye in the sky') cameras
  - IP/network cameras with remote control (tilt, pan and zoom)
  - Any wireless cameras (usually retained only for special security ['spying'/special investigation] work)
- Comms including PA
- EAS systems
- Key access and locking systems for guest rooms – including card-based RFID systems offering controlled access to (for example) elevators, gymnasium, and other restricted internal areas
- Motion sensors
- On-premise safes – including office and guest room safes
- Vehicle alarms
- Internet security.

Testing 'sectors'

Testing 'sectors' refers to the practice of testing, checking and verifying the operation of a system in a defined location/space.

The designation of a sector will be determined by management in conjunction with security consultants and the people who install and commission the systems.

A sector can be internal of external and may relate to:

- Certain entries and exits
- Car parks
- A particular room or passageway
- A department
- A group of rooms or facilities – a general area
- A specified type of system.

Standard practice is to:

- Test/check one system at a time
- Test/check one sector at a time
- Record all testing/checking procedures and the results/outcomes.

Testing 'according to assignment instructions'

Testing to assignment instructions refers to:

- Using the tools and equipment for undertaking designated maintenance activities/jobs – including having access to and using:
  - Service/Repair manuals
  - Diagnostic information
- Conducting checks/tests of sectors and systems in accordance with pre-determined schedules and testing regimes – these are the standard testing requirements for systems/technologies conducted on a regular and ongoing basis
- Conducting one-off checks such as:
  - Directed by management – perhaps in response to a problem situation or a concern they have about the operation/coverage of the system
  - Deemed necessary on the basis of (for example):
  - A system malfunction
  - A breach of security
  - Personal observations/monitoring which indicate a potential issue/cause of concern
- Applying certain types of checking/testing such as:
  - Perimeter vulnerability tests

- Penetration testing
- PCI compliance testing
- Cable testing.

The use of 'assignment instructions' demonstrates you do not have the authority to simply interfere with security systems: you can only take action:

- In response to an alarm – for the purpose of diagnosis/investigation
- As part of standard testing and maintenance
- For approved monitoring activities.

Activities involved

Activities involved are a mix of inspections and active testing.

All activities must comply with:

- Local legislation
- Local COPs
- Manufacturer's instructions.

Inspections

These are physical inspections to (for example) determine:

- Fire extinguishers are actually located where they are supposed to be – and have not been moved, stolen or disconnected
- Extinguishers have been services according to their service schedule
- Smoke detectors have not been painted over as part of a refurbishment of the property
- Nozzles of fire hoses are still in place and have not been stolen
- Security mirrors are still correctly positioned and angled – and allow operators to view hidden areas
- Cleanliness of lenses on cameras and domes
- Components showing signs of leaks, looseness, corrosion, damage, interference or anything out of the ordinary.

Active testing

These tests are system-specific and will address and have a focus on the initiating devices (the system components which will trigger an alarm – items such as smoke detectors, heat detectors and beam detectors).

Issues addressed as part of active testing include testing:

- Actual response and sensitivity of smoke and heat detectors – using (for example) commercial aerosol products
- Tilt, pan and zoom facilities of relevant cameras

- Freedom from physical impediment in line-of-sight cameras
- Quality of pictures from CCTV cameras
- Recording quality and capacity of CCTV
- Flow rates of hydrants and hoses
- Scanners using a sample 'test scan' package or item
- Lesser used elements and functions of systems – these items are not frequently used and may fall into disrepair: it is important they are tested to ensure operational effectiveness because many of these components (while only used infrequently) are extremely important when they are needed

- Locks – all types, all fixtures and fittings
- All audible alarms – this should be done 'remotely' and 'locally'. Remotely refers to initiating an alarm at the control panel and verifying the required indicator is showing. Locally refers activating the alarm at the point where the initiating device is located (by, for example, opening an alarmed door to verify the alarm sounds) and verifying:
  - The alarm has sounded at the door
  - The control panel is indicating the alarm has been activated
- Operation of all shut-off valves – for gas, water and electricity
- All visual alarms – by physically observing they are working as required and not just assuming they are working because an indicator light in the control room says they are

- All levels of alarms – for example alarms may have different sequences (or tones) to indicate various levels of alert, such as:
  - Stage 1 – indicates (for example) 'There is a fire in the building but there is no need to evacuate'
  - Stage 2 – indicates 'There is a fire in the building and there may be a need to evacuate'
  - Stage 3 – indicates 'Evacuate now'.

Standard requirements

The following are SOP when undertaking testing of systems:

- Certified and accredited testers must be used – where specified by law or manufacturer's instructions
- Notify the authorities (police and fire) you are conducting a test (or a drill) – to avoid an emergency response when there is no need
- Notify any remote monitoring sites you are conducting a test
- Advise patrons in advance of any test which requires an audible or visual signal – to prevent worry and avoid panic

- Conduct tests in accordance with specifications for each system as required by the manufacturer, supplier and/or installer. In practice this means tests of different types are usually conducted:
  - Quarterly
  - Half-yearly
  - Annually.
- Advise and involve external security support companies where faults or discrepancies are identified as a result of the testing procedures
- All problems must be investigated and remedied
- Ensure any maintenance requirements identified as part of the testing program are addressed – by internal service or through using external service providers

- Testing activities MUST be recorded – detailing:
  - Dates and times
  - Items or systems tested
  - Nature of tests conducted
  - Results of tests – including (as appropriate) hard copy data from the system
  - Names of those who conducted tests.

Work Projects

It is a requirement of this Unit you complete Work Projects as advised by your Trainer. You must submit documentation, suitable evidence or other relevant proof of completion of the project to your Trainer by the agreed date.

2.1 Visit a venue, interview an appropriate person and prepare a list which:

- Identifies/describes the PPE used
- Explains how to use each item
- Describes requirements for maintaining each identified item.

2.2. Interview an appropriate person at a venue and prepare a report which details internal requirements relating to:

- Operation of security equipment and systems
- Actions Security Officers are authorised to take and those they are prohibited from taking
- The way in which (demeanour/manner) Security Officers are required to undertake their role and interact with the public
- Monitoring of surveillance equipment
- Testing alarms.

Summary

Operate security equipment

When operating security equipment:

- Make sure you use/wear all mandatory PPE
- Use a duty/utility belt to help with EDC items
- Maintain PPE as required/necessary
- Comply with all legislated requirements
- Realize the limitations of the action you can take
- Remember you are not a police officer
- Follow manufacturer's instructions when operating equipment
- Be controlled and restrained in your interactions with people
- Follow all internal SOPs/protocols
- Monitor all equipment. systems and displays/boards
- Maintain situational awareness
- Inspect and actively test equipment and systems in accordance with established schedules
- Record details and results of all tests and inspections
- Respond as required to all issues identified by inspections and tests.

Element 3:
Maintain security equipment and resources

3.1 Return security equipment to operational condition

Introduction

Given the essential roles performed by security equipment it is crucial to return all items to operational condition when damage or a malfunction is identified.

This section identifies the importance of this action and describes what is involved.

Importance of this step

Returning security equipment back to full operational status is important for the following reasons:

- To optimize and maintain security coverage as intended for the venue
- To maintain trust and confidence of guests
- To give staff a sense of well-being and security
- To discharge Duty of Care obligations
- To deliver on promises made about a safe and secure environment
- Because many criminals include disabling of security equipment as a fundamental part of their plan
- To reduce cost of loss (to patrons and venue) occasioned by events which occur when – or because – security systems and equipment are not operational.

Possible action to take

As a Security Officer un-trained in servicing or repairing systems and equipment your practical actions in returning items back to operational condition when damage or a fault is detected are very limited.

Options include:

- Notifying others to come and assess the situation and make necessary repairs – this may mean contacting Head Office, the manufacturer, your Maintenance department or a designated service provider or security technician or consultant. Remember you can only do this within your designated scope of authority so in some cases you will have to report or refer the issue for someone else to action

- Obtaining a replacement item – and taking the faulty/damaged item away, out-of-service or off-line
- Using common sense combined with any relevant experience and training to (for example):
  - Remove whatever is causing the problem, fault or damage, and then testing the item
  - Re-set the piece of equipment or system – where this facility exists: non-operational security equipment can sometimes be the result of some internal problem or conflict
  - An option to re-setting the item (where no re-set facility exists) may be to turn it off, wait 20 seconds, and then turn it back on again

- Taking whatever action appears logical at the time and given the circumstances you are faced with
- Implementing an alternative security option – for example:
  - If a window is broken (giving rise to the potential for unauthorized entry) you might stay on site (as a guard) until the broken window is shuttered or replaced
  - If the belt scanner is not working then you may implement scanning using hand-held wands.

Follow-up action

Whenever you identify a piece of security equipment which was not operating correctly you will need to follow one or more protocols as established by the workplace.

These can include:

- Remaining at the site/location for a period to verify what you have done really has fixed the problem
- Returning at a later time to check the item you fixed and returned to service is still working properly
- Reporting the issue verbally to your supervisor – see section 3.3
- Completing designated internal form/report flagging the incident and the action you took
- Arranging for extra security staff to patrol/attend the location to provide extra human resources to supplement the failed physical resources.

3.2 Clean, maintain and store security tools and equipment

Introduction

Security staff have responsibility for cleaning, basic maintenance and storing of security tools and equipment.

Cleaning equipment

It is necessary to clean security equipment/items to:

- Optimize operational performance
- Enhance appearance of items so they look good to customers/guests. There is no doubt guests infer things from the appearance/condition of security equipment. They have much more confidence in the venue and its ability to safeguard them where they see clean and properly maintained security equipment

Cleaning instructions for most (small) items of security equipment are to be found in the User Manual/Instruction Manual which accompanies purchase of the item.

Cleaning basics are:

- Use only designated chemicals for cleaning – certain items demand certain cleaning agents
- Use only designated cleaning products – some items can be cleaned using a cloth and some (for example) require a brush
- Adhere to required cleaning schedule for each item – if a cleaning schedule does not exist, develop one
- Cleaning of items should be allocated to specified staff members – so everyone knows what they have responsibility for and to ensure no item is omitted from the cleaning regime
- Cleaning is a task which should be given the appropriate time – this means cleaning of security items needs to be time-tables into normal duties and not treated as something which is done ‘if there is time’
- Cleaning of many items should be scheduled and undertaken during quiet times – this can mean it needs to be done during ‘low’ periods and/or at night.

Online information

Visit the following for examples of specific cleaning advice:

- http://thehitechzone.com/surveillance-earpiece-2/tech-tip-how-to-clean-your-surveillance-earpiece-tube/.

Maintaining equipment

Always:

- Follow manufacturer's instructions when undertaking maintenance
- Stay within your designated scope of authority when taking action
- Ask for assistance when unsure about what to do
- Be prepared to obtain qualified help when faced with an uncertain or difficult situation.

Generic maintenance activities can include:

- Regular/scheduled cleaning – it is critical you understand how important clean equipment is to its effective operation
- Lubricating moving parts
- Changing batteries
- Making minor modifications and adjustments
- Tightening screws, nuts and bolts, fixtures and fittings, panels, straps and similar
- Undertaking basic repairs
- Replacing parts commonly subject to wear – such as O-rings, washers, belts, globes, fuses
- Providing service designed to prevent 'wear and tear' on the equipment – so it can remain in service and to reduce the potential for, and amount of, down-time

- Completing required documentation to record work performed, time taken and parts used.

Note there can be supplementary requirements for some maintenance activities – for example:

- You may be required to be a fully-licensed electrician in order to undertake some maintenance work
- You may have to be certified by a manufacturer before you can maintain certain equipment without voiding warranties or guaranties.

Storing equipment

The fundamentals of storing security tools and equipment are:

- Store items immediately after cleaning and maintenance has been completed
- Return items to their individual containers, where appropriate
- Locate each and every item in its designated location
- Update internal storage documentation
- Secure the storage area.

3.3 Report faulty or damaged security equipment and items

Introduction

A vital element of maintaining security equipment and resources is reporting damaged and faulty items in situations where you are unable to fix them.

This section reinforces why this is necessary, identifies what to report and describes reporting options.

Importance of reporting

Faulty or damaged security equipment and items must be reported for one or more of the following reasons:

- So arrangements can be made to initiate required repairs, service or other action (such as replacement of items, purchase of additional items or purchase of different types of items)
- For insurance purposes – so an insurance claim can be made'
- In order the business can rely on the protection afforded by product warranty or guaranties
- To enable generation of an historic body of evidence about faults and damage to security items – which may be used as the basis for preventing future events
- In order a claim for reimbursement may be made against a customer/guest who has intentionally damaged an item
- To obtain one-off permission for you to take action in excess of your standard scope of authority to effectively address the identified situation
- In order to comply with internal policies related to reporting of issues
- To share information with other staff so they are aware of the situation, possible cause and item/s involved.

Reporting

Immediacy of reporting

It is standard procedure for you to have to report faulty or damaged security immediately so action can be taken to address the situation, and so other staff are aware of the problem and the extent to which normal security has been compromised.

This will mean using your radio to communicate with the 'appropriate person'.

This is a mandatory requirement.

'Appropriate person'

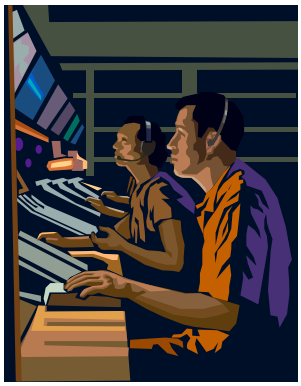
The appropriate person to report to will often depend on the time of day the problem is identified.

For example a fault at 2:00AM may require you to report:

- Direct to the external security consultant/provider so they can initiate action to fix the problem
- To the Night Auditor.

In other circumstances/at other times you may be required to report to:

- The control room
- Your supervisor
- Head of Security
- Duty manager
- Head office
- Maintenance department
- The owner.



Reporting options

Options for reporting damaged or faulty security items are:

- Using two-way radio
- Using internal telephone system
- Using cell phone
- Making a face-to-face report – which can occur:
  - On-site when the appropriate person has responded to a radio or phone call and attended the location
  - On your return to the control room after the situation has been resolved
  - At end-of-shift as part of the standard de-briefing
- Completing documentation after the event to record full details – such as:
  - Incident Report
  - Maintenance Request.

What to report

The details of the report will, obviously, reflect the individual fault or damage situation but the following generic requirements will always apply:

- Name/type of item
- Identification of product/serial number
- Description of identified problem
- Known cause/s – if any, including names of anyone involved in causing the fault/damage

- Urgency involved in returning item to full operational status
- Details of any action taken by you on-the-spot to try to fix the problem/fault/damage
- Explanation of action taken to maintain security at the site
- Suggestions for action to take – this is often extremely beneficial as you can be expected to have a detailed knowledge of the venue, the situations, possible threats and practical options for addressing the problem..

3.4 Arrange back-up systems for faulty or damaged security equipment and items

Introduction

In some situations there can be a need to arrange back-up systems for faulty or damaged security equipment/items.

This section discusses this potential requirement.

When this action is necessary

You will need to arrange back-up items or systems where damaged or faulty systems cannot be fixed:

- By yourself on-the-spot
- By others in the workplace – such as qualified technicians or maintenance staff
- By external providers – who have attended and inspected/diagnosed the problem.

The reality of the situation

In most cases venues do not have back-up ‘security systems’.

This is because:

- They are too expensive to duplicate
- They are too complex – in terms of how and where they are installed.

Instead venues will probably have replacement ‘components’ (such as spare/replacement cameras, spare detectors, spare VDUs or an assortment of general ‘spare parts’).

Context

In this context ‘security systems’ refers to:

- Large items of security equipment such as:
  - Walk-though scanners
  - Conveyor belt baggage scanners/X-ray machines
- Fire monitoring systems
- Intruder or intrusion detection systems.

Practical responses

Given the usual lack of a full back-up system on site, when 'the system' fails you will need to:

- Be alert to the possibility the system failure was the result of an intentional act caused by a would-be offender – a standard response to system failure is to enhance on-the-ground, eyes-on security
- Run immediate system diagnostic checks – many systems have the capacity to self-diagnose a problem and report on what can be done to fix the problem
- Contact the manufacturer/provider:
  - Some systems and equipment can be remotely interrogated to identify faults and problems and some (relatively few) can even be repaired from this remote location)
  - They may be able to provide over-the-phone advice about what to do to (try to) fix the problem
  - To initiate a service call to address the situation

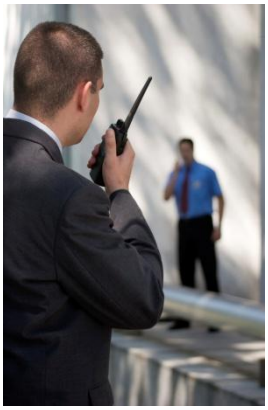
- Contact remote control rooms which may be linked to/monitoring the systems – in order to:
  - Determine if they have the same indicators of malfunction you are experiencing
  - Identify if they can suggest remedial action which may be taken to retrieve the situation
- Contact the external security company used by your venue – this can be a formal SOP where systems fail so as to:
  - Advise them of the situation
  - Call in extra security officers to provide additional security coverage
- Contact the authorities – this can mean:
  - Notifying the police where intruder systems have gone down
  - Advising the fire authorities win situations where the fire monitoring system has failed

- Initiate an alternate security strategy to deal with the situation – most venues will have a set of contingency plans developed to deal with situations where major security systems fail.

  Generic options include:
  - Increased foot patrols
  - Higher levels of awareness
  - Increased checks and inspections.

Important considerations

In these circumstances:



- Respond quickly
- Stay within your designated scope of authority … but you will be expected to exercise common sense and initiative: this is a fine balancing act but one management will expect you to discharge
- Notify others – communication with internal and external personnel is critical
- Be ready to limit normal activities – as required in order to respond effectively. This may include:
  - Closing some entry and exit points – or making sure there is only one ingress/egress point
  - Prohibiting vehicle access to nominated areas
  - Restricting access to high-risk areas
- Record the situation – take notes of what happened and your actions; note times and who was involved; use cameras to record physical evidence
- Actively participate in the de-brief which normally follows such situations – to provide information which may be able to be used to:
  - Prevent a recurrence
  - Enhance future responses to similar situations.

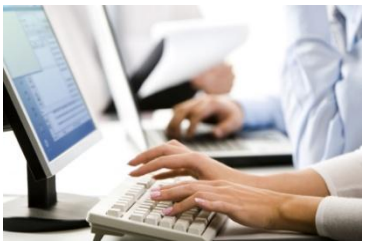
3.5 Complete internal records and reports relating to security

Introduction

At all times there is a need to complete internal records and reports as required by the venue.

This section identifies examples of documentation which may need to be completed and describes the matters which need to be recorded.

Background information



In relation to the need to complete internal records and reports:

- These vary between venues – what is required in one venue is not required in another; what does not have to be reported and recorded in one premises does have to be reported and recorded elsewhere
- It is important to complete the documents in a timely manner – in practice this means filling in reports and records ‘immediately’ after an incident, event or nominated activity
- Completed documentation needs to be ‘forwarded’ – there is always a need to file a form or hand it in to a designated person/department

- Accuracy is vital – it is essential you take the time to make sure all the details (information as well as statistical data) is correct in every aspect
- Obtain necessary in-house training – all venues will provide advice and instruction on:
  - Which documents to use when a report/record is required
  - How to complete the required
  - When to complete them
  - What to do with them when they are completed
- Make an effort to look at records/reports others have completed – to get a 'feel' for how they complete them, the language and phrases used, and the detail included
- Keep a copy of any records and reports you complete – for your own records 'after the event'
- Seek advice – when uncertain about:
  - Whether a record or report is required
  - Details and information required.

Documentation format

Required reports and records may be:

- Paper-based – meaning there is an actual piece of paper which has to be completed
- Electronic – meaning you will have to access a computer and complete the details ('required fields').

Examples of reports and records

Types of reports and records will vary between venues.

Some of the forms identified below may be combined by some operators into the one document which then becomes a multi-purpose form.

Reports and records you may be required to complete can include:

- Communications book – used by venues to facilitate communication between staff who work different shifts/days.
- Maintenance Request forms – also known in some venues as Maintenance Requisitions
- Maintenance reports – detailing repairs, service and maintenance on items specifying what was done, when it was done and who did it. This form is required when maintenance is undertaken by internal staff or an external provider
- Time sheets – detailing hours worked for a shift: a time clock may replace the need to complete a paper-based time sheet
- Task assignments – at the end of the allocated assignment
- Job cards – when allocated work (inspections, repairs, replacements) have been finalised this record will detail:
  - Who did the job
  - Time taken

  - Materials used
  - Parts and components replaced.
  - These details enable costing of work done

- Patrol reports – at the end of vehicle and foot patrols completed at the end of the patrol or end-of-shift to record times and routes as well as operational details
- Suspicious person report – completed at the end of the patrol, end-of-shift or after having responded to a call from venue staff to investigate
- Incident report – to record details relating to an incident which has occurred in the venue
- CCTV surveillance records – to identify discs/tapes stored/maintained for different dates, times and locations/cameras
- Alarm reports – identifying activated alarms, locations, times and causes including false alarms
- Response reports – detailing action taken in response to alarms and calls for assistance
- Equipment faults log – this is used to report operational faults in systems and equipment and to record action taken to record diagnoses
- Testing and inspection records – which:
  - Provide evidence of inspections/tests having been undertaken
  - Highlight areas where problems/issues have been identified for further action/follow-up
- Witness statements – taken when members of the public are prepare to make statements regarding what they observed when an event, incident or offence took place. Members of the public, customers or guest are under no obligation to make witness statements
- Recommendations for action – this is a form allowing staff to formally convey suggestions and ideas for issues such as:
  - Changes to SOPs
  - Introduction of new SOPs
  - Replacement of items
  - Disposal of faulty or damaged equipment
  - Purchase of new or different items and equipment.
- Request for training – identifying the training required (such as ‘initial training’, ‘top-up training’ or ‘refresher training’) and the items (equipment and/or systems) involved. This training request may also identify ancillary areas in which training is required – these areas may include:
  - First aid
  - Maintenance and service.

Work Projects

It is a requirement of this Unit you complete Work Projects as advised by your Trainer. You must submit documentation, suitable evidence or other relevant proof of completion of the project to your Trainer by the agreed date.

3.1 Contact a provider of security equipment or a manufacturer (either in person, through a third party or online) and obtain and submit:

- User manual/Service manual for one item of security equipment
- Cleaning and maintenance schedule/requirements for the item.

3.2. Visit a venue, talk to an appropriate person and prepare a report detailing:

- How Security Staff report faulty or damaged security equipment and items
- Who those reports are made/forwarded to
- The arrangements in place for organising/obtaining back-up for faulty or damaged security equipment and items
- Internal records and/or reports that Security Officers need to complete as part of their responsibilities identifying when and why these documents need to be completed.

Summary

Maintain security equipment and resources

When maintaining security equipment and resources:

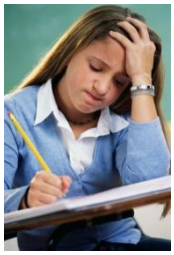
- Follow manufacturer's instructions
- Adhere to maintenance schedules
- Stay within your designated scope of authority
- Arrange alternate, substitute or back-up actions or plans where items cannot be repaired or returned to full operational status
- Conduct preventative maintenance as required
- Inform/advise nominated external sources when a problem occurs
- Realize cleaning is a primary maintenance activity for equipment/items
- Report and/or refer any situations you cannot fix
- Learn the SOP back-up protocols and plans where security equipment and systems are compromised
- Adjust standard security arrangements to respond effectively to identified faults and damage to security equipment
- Complete internal records and reports as required.

Presentation of written work

1. Introduction

It is important for students to present carefully prepared written work. Written presentation in industry must be professional in appearance and accurate in content. If students develop good writing skills whilst studying, they are able to easily transfer those skills to the workplace.

2. Style



Students should write in a style that is simple and concise. Short sentences and paragraphs are easier to read and understand. It helps to write a plan and at least one draft of the written work so that the final product will be well organized. The points presented will then follow a logical sequence and be relevant. Students should frequently refer to the question asked, to keep 'on track'. Teachers recognize and are critical of work that does not answer the question, or is 'padded' with irrelevant material. In summary, remember to:

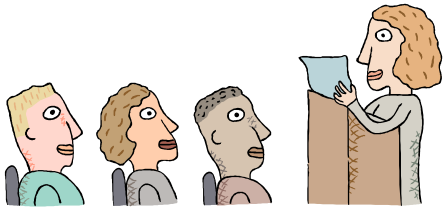
- Plan ahead
- Be clear and concise
- Answer the question
- Proofread the final draft.

3. Presenting Written Work

Types of written work

Students may be asked to write:

- Short and long reports
- Essays
- Records of interviews
- Questionnaires
- Business letters
- Resumes.



Format

All written work should be presented on A4 paper, single-sided with a left-hand margin. If work is word-processed, one-and-a-half or double spacing should be used. Handwritten work must be legible and should also be well spaced to allow for ease of reading. New paragraphs should not be indented but should be separated by a space. Pages must be numbered. If headings are also to be numbered, students should use a logical and sequential system of numbering.

Cover Sheet

All written work should be submitted with a cover sheet stapled to the front that contains:

- The student's name and student number
- The name of the class/unit
- The due date of the work
- The title of the work
- The teacher's name
- A signed declaration that the work does not involve plagiarism.

Keeping a Copy

Students must keep a copy of the written work in case it is lost. This rarely happens but it can be disastrous if a copy has not been kept.

Inclusive language

This means language that includes every section of the population. For instance, if a student were to write 'A nurse is responsible for the patients in her care at all times' it would be implying that all nurses are female and would be excluding male nurses.

Examples of appropriate language are shown on the right:

Mankind	*Humankind*
Barman/maid	*Bar attendant*
Host/hostess	*Host*
Waiter/waitress	*Waiter or waiting staff*

Recommended reading

Note: all Recommended Reading is sourced from 'Trove: National Library of Australia' at http://trove.nla.gov.au/.

2010; *Security equipment catalogue*; Security Construction and Equipment Committee, Canberra

Australian Security Intelligence Organisation 2004; *Security equipment catalogue*; Australian Security Intelligence Organisation, Canberra

Bergquist, Carl J 2002; *Guide to electronic surveillance devices;* Thomson/Delmar, Clifton Park, N.Y

Brookes, Paul 2001; *Electronic surveillance devices;* 2nd ed, Newnes, Oxford

Clifton, Darrell 2012; *Hospitality security: managing security in today's hotel, lodging, entertainment, and tourism environment*; CRC Press, Boca Raton, FL

Fischer, Robert J & Halibozek, Edward P & Walters, David, 1963- 2013; *Introduction to security*, 9th ed; Elsevier, Amsterdam; New York

National Burglar and Fire Alarm Association (U.S.) & Security Equipment Industry Association 1971; *Security distributing & marketing;* Cahners Pub. Co, Boston, MA

Singapore Hotel Association & Singapore. Police Force & Singapore. National Crime Prevention Council 2003; *Hotel security: the SHA manual*; SHA Hospitality Press, Singapore

Smith, Harry (Harold F.) 1993; *Hotel security*; C.C. Thomas, Springfield, Ill., U.S.A

Trainee evaluation sheet

Operate basic security equipment

The following statements are about the competency you have just completed.

Please tick the appropriate box	Agree	Don't Know	Do Not Agree	Does Not Apply
There was too much in this competency to cover without rushing.	☐	☐	☐	☐
Most of the competency seemed relevant to me.	☐	☐	☐	☐
The competency was at the right level for me.	☐	☐	☐	☐
I got enough help from my trainer.	☐	☐	☐	☐
The amount of activities was sufficient.	☐	☐	☐	☐
The competency allowed me to use my own initiative.	☐	☐	☐	☐
My training was well-organized.	☐	☐	☐	☐
My trainer had time to answer my questions.	☐	☐	☐	☐
I understood how I was going to be assessed.	☐	☐	☐	☐
I was given enough time to practice.	☐	☐	☐	☐
My trainer feedback was useful.	☐	☐	☐	☐
Enough equipment was available and it worked well.	☐	☐	☐	☐
The activities were too hard for me.	☐	☐	☐	☐

The best things about this unit were:

The worst things about this unit were:

The things you should change in this unit are:


William
Angliss
Institute
Specialist centre
for foods, tourism
& hospitality
asean
Australian
AID