



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC2019A Monitor biometric equipment and systems

Release: 1

CPPSEC2019A Monitor biometric equipment and systems

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to monitor the operational effectiveness of a range of biometric equipment and systems in a workplace environment.

It requires the ability to monitor and respond to biometric equipment and systems data and information, receive and verify data, identify discrepancies and potential breaches of security, and implement appropriate responses. It also involves change of shift duties including the processing and maintenance of workplace information.

An understanding of the operating principles of biometric equipment, systems and technology is also required as well as the ability to interpret and apply effective principles and requirements relating to confidentiality, privacy and security in own work.

This unit may form part of the licensing requirements for persons engaged in security operations involving the use of biometric equipment and systems in those states and territories where these are regulated activities.

Application of the Unit

Application of the unit

This unit of competency has application in those roles involving the operation of biometric equipment and systems to maintain security. Competency requires legal and operational knowledge applicable to relevant sectors of the security industry. The knowledge and skills described in this unit are to be applied within relevant legislative and organisational guidelines.

Licensing/Regulatory Information

Refer to Unit Descriptor

Pre-Requisites

Not Applicable

Employability Skills Information

Employability skills This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Elements describe the essential outcomes of a unit of competency. Performance criteria describe the required performance needed to demonstrate achievement of the element. Where ***bold italicised*** text is used, further information is detailed in the required skills and knowledge section and/or the range statement. Assessment of performance is to be consistent with the evidence guide.

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
<p>1 Apply the principles of confidentiality, privacy and security in own work.</p>	<p>1.1 Applicable <i>Occupational Health and Safety (OHS)</i>, <i>legislative</i> and <i>organisational requirements</i> relevant to <i>monitoring biometric equipment and systems</i> are identified and complied with.</p> <p>1.2 Relevant <i>privacy legislation</i> and codes of ethics relevant to the workplace application of biometric technology are accessed and interpreted.</p> <p>1.3 Privacy and confidentiality of client data and information, verbal and written, is securely maintained in accordance with legislative and organisational requirements.</p> <p>1.4 Potential confidentiality issues are promptly identified and clarified as required with <i>relevant persons</i>.</p> <p>1.5 Effective <i>communication</i> and <i>interpersonal techniques</i> are used that reflect sensitivity to individual <i>social and cultural differences</i>.</p>
<p>2 Prepare to monitor data and information.</p>	<p>2.1 <i>Work order</i> instructions and information are reviewed and confirmed as required with relevant persons in accordance with workplace procedures.</p> <p>2.2 Location and <i>mode</i> of biometric equipment and systems are identified and confirmed in accordance with workplace procedures.</p> <p>2.3 <i>Resources</i> relevant to work requirements are identified and organised in accordance with workplace procedures.</p> <p>2.4 <i>Administrative</i> requirements are identified and arranged in accordance with organisational requirements.</p> <p>2.5 Potential and existing <i>risks</i> and <i>hazards</i> in the work area are identified and controlled in accordance with OHS and organisational requirements.</p>
<p>3 Monitor data and information.</p>	<p>3.1 All work is conducted using established <i>ergonomic</i> practices in accordance with OHS and organisational requirements.</p> <p>3.2 <i>Enrolment</i> procedures are conducted in a systematic manner to ensure accuracy and currency of data in accordance with organisational requirements and standards</p> <p>3.3 Data and information is routinely monitored for consistency and compliance with established authorisations and standards.</p> <p>3.4 Data and information is collected and organised in a logical and sequential manner in accordance with workplace procedures and standards.</p>

ELEMENT	PERFORMANCE CRITERIA
	3.5 Data and information is checked for accuracy, relevance and compliance with security, legal and privacy requirements.
	3.6 Received data and information is processed and securely stored in accordance with workplace procedures.
	3.7 Errors or irregularities in received data and information are identified and reported in accordance with workplace procedures.
	3.8 Potential breaches of information security are identified and promptly reported to relevant persons in accordance with workplace procedures.
4 Complete monitoring activities.	4.1 Change of shift procedures are complied with to ensure monitoring continuity is maintained in accordance with workplace procedures.
	4.2 Identified faults or deficiencies in biometric equipment and systems are identified and reported in accordance with workplace procedures.
	4.3 Monitoring operations are reviewed and findings are accurately documented and processed in accordance with workplace procedures.
	4.4 Recommendations or identified opportunities to improve monitoring operations are recorded and forwarded to relevant persons to inform future practice.
	4.5 Records and reports are completed and maintained in accordance with legislative and organisational requirements.

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

This section describes the skills and knowledge and their level required for this unit.

Required skills

- accurately and securely maintain records, reports and other workplace information
- comply with applicable confidentiality and privacy requirements
- comply with legislation, regulations, standards, codes of practice relevant to monitoring biometric equipment and systems
- conduct change of shift procedures
- identify and control risks and hazards
- identify basic faults or deficiencies in operation of biometric equipment and

REQUIRED SKILLS AND KNOWLEDGE

systems

- identify potential breaches of security
- monitor biometric data and information and identify errors
- organise work priorities and arrangements and complete work tasks within designated timeframes
- read and interpret data, information and instructions
- relate effectively to people from a range of social, cultural and ethnic backgrounds and varying physical and mental abilities
- resolve problems within scope of responsibilities
- select and use equipment and technology appropriate to the work task
- undertake effective enrolment of biometric and biographical data
- use appropriate communication and interpersonal skills including speaking clearly and questioning
- written communication skills sufficient to document findings and complete relevant records and reports.

Required knowledge

- applicable commonwealth, state or territory legislation, regulations, standards and codes of practice relevant to the full range of processes relating to monitoring biometric equipment and systems
- appropriate mathematical procedures for estimating, measuring and calculating.
- biometric equipment and system configurations and programs
- biometric terminology
- change of shift practices and procedures
- ergonomic and safe working practices and procedures
- established threshold levels and their impact on security
- information security management processes
- initial enrolment procedures
- monitoring and response requirements
- operational principles of information technology
- organisational standards, policies and procedures for monitoring biometric equipment and systems
- organisational structure procedures for recording, reporting and maintaining workplace information
- principles of cultural diversity and access and equity
- types, functions and parameters of biometric equipment and systems and databases
- verification procedures and requirements for confirming authenticity of received information
- virus protection procedures
- workplace communication channels, protocols and procedures.

Evidence Guide

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Critical aspects for assessment and evidence required to demonstrate competency in this unit

A person who demonstrates competency in this unit must be able to provide evidence of:

- complying with applicable legislation and codes of ethics applicable to privacy and client confidentiality
- complying with organisational policies and procedures, including OHS, relevant to biometric work tasks
- implementing and monitoring change of shift procedures and accurately completing and maintaining documentation, records and reports
- organising resources and relevant authorisations required to undertake monitoring work appropriate to type and mode of biometric equipment and system
- prioritising and responding promptly to data and information in compliance with monitoring parameters
- responding to biometric equipments and systems, data and information in a systematic manner and implementing procedures to verify accuracy and reliability of received information.

Context of and specific resources for assessment

Context of assessment includes:

- a setting in the workplace or environment that simulates the conditions of performance described in the elements, performance criteria and range statement.

Resource implications for assessment include:

- access to a registered provider of assessment services
- access to a suitable venue and equipment including biometric equipment and systems
- access to plain English version of relevant statutes and procedures
- assessment instruments including personal planner and assessment record book
- work schedules, organisational policies and duty statements.

Reasonable adjustments must be made to assessment processes where required for people with disabilities. This could include access to modified equipment and other physical resources, and the provision of appropriate assessment support.

Method of assessment	<p>This unit of competency could be assessed using the following methods of assessment:</p> <ul style="list-style-type: none"> • observation of processes and procedures • questioning of underpinning knowledge and skills.
Guidance information for assessment	<p>Assessment processes and techniques must be culturally appropriate and suitable to the language, literacy and numeracy capacity of the candidate and the competency being assessed. In all cases where practical assessment is used, it should be combined with targeted questioning to assess the underpinning knowledge.</p> <p>Oral questioning or written assessment may be used to assess underpinning knowledge. In assessment situations where the candidate is offered a choice between oral questioning and written assessment, questions are to be identical.</p> <p>Supplementary evidence may be obtained from relevant authenticated correspondence from existing supervisors, team leaders or specialist training staff.</p>

Range Statement

RANGE STATEMENT

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

<i>Occupational Health and Safety (OHS) requirements may relate to:</i>	<ul style="list-style-type: none"> • controlling and minimising risks • correct manual handling including shifting, lifting and carrying • elimination of hazardous materials and substances • identifying hazards • safety procedures for the protection of self and others • safe use and operation of equipment including <ul style="list-style-type: none"> • business technology • first aid equipment • fire safety equipment • personal protective clothing and equipment • safety equipment.
<i>Legislative</i>	<ul style="list-style-type: none"> • Australian standards and quality assurance requirements

requirements may relate to:

- award and enterprise agreements
- Compliance Policy Guidelines (CPGs)
- counter-terrorism
- general 'duty of care' responsibilities
- licensing or certification requirements
- privacy and confidentiality
- relevant commonwealth, state and territory legislation, codes and national standards for:
 - anti-discrimination
 - cultural and ethnic diversity
 - environmental issues
 - equal employment opportunity
 - industrial relations
 - OHS
- relevant industry codes of practice
- telecommunications.

Organisational requirements may relate to:

- access and equity policies, principles and practices
- business and performance plans
- client service standards
- code of conduct, code of ethics
- communication and reporting procedures
- complaint and dispute resolution procedures
- emergency and evacuation procedures
- employer and employee rights and responsibilities
- environmental management including waste disposal, recycling and re-use guidelines
- OHS policies, procedures and programs
- own role, responsibility and authority
- personal and professional development
- privacy and confidentiality of information
- quality assurance and continuous improvement processes and standards
- resource parameters and procedures
- roles, functions and responsibilities of security personnel
- standard operating procedures
- storage and disposal of information
- use and maintenance of equipment and systems.

Monitoring parameters may relate to:

- functions (alarms, system on and off, access times, levels of access, identity of users gaining access)
- integrity of biometric equipment and systems
- integrity of data and information
- recording and reporting functions

- Biometric refers to:***
- security incident and response requirements
 - a measurable physical characteristic or personal behavioural trait used to recognise the identity or verify the identity of an individual.
- Biometric equipment and systems are:***
- automated systems able to capture a biometric sample from an individual person, extract biometric data from the sample, compare the data with one or more reference templates, determine the quality of a match, and indicate whether or not an identification or verification of identity has been achieved.
- Biometric equipment and systems may include:***
- acquisition devices
 - cameras (video, infrared-enabled video, single-image)
 - chip or reader embedded in peripheral device
 - microphones
 - optical scanners
 - biometric servers
 - hardware
 - interconnecting infrastructure
 - software
 - server-based authentication software for biometric authentication and logging
 - software associated with acquisition devices.
- Privacy legislation may include:***
- Commonwealth, State and Territory Privacy Acts
 - national information privacy principles
 - national privacy principles.
- Relevant persons may include:***
- biometric technology specialists
 - clients
 - colleagues
 - information technology specialists
 - supervisor.
- Communication may be:***
- face-to-face
 - group interaction
 - in Indigenous languages
 - in languages other than English
 - oral reporting
 - participation in routine meetings
 - reading independently
 - recording of discussions
 - speaking clearly and directly
 - through the use of assistive technology
 - via an interpreter
 - visual or written

Interpersonal techniques may involve:

- writing to audience needs.
- active listening
- being non-judgemental
- being respectful and non-discriminatory
- constructive feedback
- control of tone of voice and body language
- culturally aware and sensitive use of language and concepts
- demonstrating flexibility and willingness to negotiate
- effective verbal and non-verbal communication
- maintaining professionalism
- providing sufficient time for questions and responses
- reflection and summarising
- two-way interaction
- use of plain English
- use of positive, confident and cooperative language.

Social and cultural differences may relate to:

- dress and personal presentation
- food
- language
- religion
- social conventions
- traditional practices
- values and beliefs.

Work order instructions and information may include:

- access and authorisation requirements
- incident and security risk response procedures
- location of biometric equipment and systems
- monitoring parameters and objectives
- OHS, confidentiality and other legal requirements
- personal presentation requirements
- personal protection equipment
- reporting and documentation requirements
- resource and equipment requirements
- specifications and components of biometric equipment and systems
- work tasks and schedules.

Mode may be:

- multiple (a biometric system that integrates two or more biometric technologies)
- single.

Resources may include:

- communications equipment
- computer equipment
- hardware and software
- procedural manuals

- standard operating procedures.
 - access
 - authorisations
 - licensing.
- Administrative requirements may relate to:***
- Risks*** may relate to:
- data and information
 - personnel
 - property.
- Hazards may be:***
- associated with electrical or mechanical faults
 - environmental
 - ergonomic
 - obstructive (blocked access to emergency entry and exit points).
- Ergonomic considerations may include:***
- avoiding radiation from computer screens
 - chair height, seat and back adjustment
 - footrest
 - keyboard and mouse position
 - lighting
 - noise minimisation
 - posture
 - rest periods, exercise breaks.
 - screen position
 - work station height and layout.
- Enrolment relates to:***
- the initial process of collecting biometric data from a user and storing it in a template for future comparison.
- Records and reports:***
- may be
 - computer-based
 - manual
 - other appropriate organisational communication system
 - may detail
 - activity reports
 - biometric equipment and systems specifications
 - change of shift procedures
 - data and information errors
 - faults and irregularities in operations
 - recommendations for improvements to processes
 - security incidents or breaches.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Biometrics