



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC4021A Prepare standard operating procedures for the use of biometric technology

Release: 1

CPPSEC4021A Prepare standard operating procedures for the use of biometric technology

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to research and develop standard operating procedures for the application of workplace biometric technologies.

It requires the ability to access, collate, and prepare information to instruct and govern the use and operation of a range of biometric technology in line with best practice. It involves the writing of operating procedures, monitoring and reviewing procedures, and implementing modifications as required.

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 to operating procedures.

This unit may form part of the licensing requirements for persons engaged in security operations involving biometric technology 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 preparation of standard operating procedures for the application of biometric technology 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
1 Identify requirements.	1.1 Applicable Occupational Health and Safety (OHS), legislative and organisational requirements relevant to the development of standard operating procedures for the use of biometric technology are identified and complied with. 1.2 Relevant privacy legislation and codes of ethics relevant to the workplace application of biometric technology are accessed and interpreted. 1.3 Relevant information relating to the types, modes, functions and parameters of biometric equipment and systems are accessed, reviewed and interpreted. 1.4 Industry issues and trends relevant to the use of biometric technology are researched and interpreted. 1.5 Security and safety issues, including risks and hazards, associated with the use of biometric technology are determined. 1.6 Consultative processes are conducted with relevant persons as required using effective communication and interpersonal techniques that reflect sensitivity to individual social and cultural differences.
2 Develop standard operating procedures.	2.1 Standard operating procedures are developed and presented in an appropriate format in accordance with organisational requirements. 2.2 Administrative requirements prior to commencing workplace operation are clearly and concisely detailed. 2.3 Specific safety information and instructions for the safe conduct of the workplace operation are clearly and concisely detailed. 2.4 Location and conditions where workplace operation is to be undertaken are clearly and concisely detailed. 2.5 Individual activities required to carry out and complete workplace operation are clearly and concisely detailed in a procedural manner. 2.6 Procedural operations of tools, equipment and technology relevant to workplace operation are clearly and concisely detailed.
3 Monitor and review standard operating procedures.	3.1 Standard operating procedures are distributed to relevant persons in accordance with organisational requirements. 3.2 Feedback is sought, reviewed and modifications implemented as required in accordance with workplace procedures. 3.3 Standard operating procedures are monitored to ensure compliance with applicable legislative, industry and organisational requirements.

ELEMENT

PERFORMANCE CRITERIA

3.4 Standard operating procedures are routinely monitored against changes in biometric technologies to maintain validity and effectiveness.

3.5 **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
- coaching and mentoring to provide support to colleagues
- comply with applicable confidentiality and privacy requirements
- comply with legislation, regulations, standards, codes of practice relevant to the development of standard operating procedures for the use of biometric technology
- evaluate standard operating procedures
- make effective decisions
- organise work priorities and arrangements and complete work tasks within designated timeframes
- read and interpret technical information including plans, designs and specifications
- relate effectively to people from a range of social, cultural and ethnic backgrounds and varying physical and mental abilities
- research, analyse and present information
- resolve problems
- 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 negotiation
- write standard operating procedures
- written communication skills sufficient to complete relevant records and reports.

Required knowledge

- applicable commonwealth, state or territory legislation, regulations, standards and codes of practice relevant to workplace biometric technology
- appropriate mathematical procedures for estimating, measuring and calculating
- ergonomic and safe working practices and procedures
- established threshold levels and their impact on security
- industry codes and best practice relating to the implementation and use of

REQUIRED SKILLS AND KNOWLEDGE

biometric technology

- initial enrolment procedures
- operational principles of information technology
- organisational procedures for recording, reporting and maintaining workplace information
- organisational standards, requirements, policies and procedures for the development of standard operating procedures for the use of biometric technology
- principles of cultural diversity and access and equity
- problem identification and resolution procedures
- procedural writing techniques
- processes for the management of enrolment data
- range of applications for biometrics and their associated disadvantages
- types, functions and parameters of biometric technologies
- 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:

- accessing, reviewing and interpreting legal, safety, privacy and organisational requirements, policies and procedures relevant to the use of biometric technology in the workplace
- 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
- preparing and organising information, and writing in a clear, concise and comprehensive manner procedural functions involved with a specific workplace operation
- routinely monitoring changes to biometric technologies and systems, assessing results against standard operating procedures and workplace application, and implementing modifications as required.

Context of and specific resources for

Context of assessment includes:

- a setting in the workplace or environment that simulates the

assessment

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
- 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	This unit of competency could be assessed using the following methods of assessment: • observation of processes and procedures • questioning of underpinning knowledge and skills.
Guidance information for assessment	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. 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. Supplementary evidence may be obtained from relevant authenticated correspondence from existing supervisors, team leaders or specialist training staff.

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>	• controlling and minimising risks • correct manual handling including shifting, lifting and carrying • elimination of hazardous materials and substances • identifying hazards • safe use and operation of equipment including • business technology • first aid equipment • fire safety equipment • personal protective clothing and equipment • safety equipment • safety procedures for the protection of self and others.
<i>Legislative requirements may</i>	• Australian standards and quality assurance requirements • award and enterprise agreements

relate to:

- 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.

Standard operating procedures are:

- established procedures specific to a given workplace operation that describe the activities necessary to use biometrics technology including staff training requirements, business processes and procedures relating to the use of biometrics, and requirements for enrolment, operation and maintenance of the biometrics system.

Biometric refers to:

- a measurable physical characteristic or personal behavioural trait used to recognise the identity or verify the identity of an individual.

Biometric technologies include:

- facial recognition
- fingerprint recognition
- hand geometry
- iris recognition
- retina recognition
- signature recognition
- vein recognition
- voice recognition.

Privacy legislation may include:

- Commonwealth, State and Territory Privacy Acts
- national information privacy principles
- national privacy principles.

Modes may be:

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

- single.

- 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.
- Risk relates to:***
- the chance of something happening that will have an impact on objectives.
- Risks may relate to:***
- data and information
 - personnel
 - property.
- Hazards may be:***
- associated with electrical or mechanical faults
 - environmental (improper use of materials and chemicals)
 - ergonomic (improper manual handling methods)
 - obstructive (blocked access to emergency entry and exit points).
- Relevant persons may include:***
- biometric technology specialists
 - clients
 - colleagues
 - external consultants
 - information technology specialists
 - manager.
- 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 • writing to audience needs.
<i>Interpersonal techniques may involve:</i>	• 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.
<i>Social and cultural differences may relate to:</i>	• dress and personal presentation • food • language • religion • social conventions • traditional practices • values and beliefs.
<i>Appropriate format may include:</i>	• formats that cater for those with special needs for example, producing documents in large print.
<i>Administrative requirements may relate to:</i>	• access • authorisations • licensing.
<i>Safety information and instructions may detail:</i>	• correct waste disposal guidelines • hazards and associated risks • maintaining a safe work area • personal protective equipment and clothing requirements • precautions to be undertaken before commencing the workplace operation • ways of minimising risk.
<i>Records and reports:</i>	• may be • computer-based

- manual
- other appropriate organisational communication system
- may detail
 - assessment outcomes
 - legislative, regulatory and OHS issues
 - reviews and modifications undertaken
 - workplace operation including specific work tasks.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Biometrics