



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC3023A Coordinate biometric equipment and systems

Release: 1

CPPSEC3023A Coordinate biometric equipment and systems

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to coordinate processes for the implementation of biometric equipment and systems in a workplace environment.

It requires the ability to determine requirements for biometric equipment and systems based on an evaluation of risk assessment information, existing architecture, and security requirements. It involves organising schedules, allocating roles and responsibilities, and applicable security authorisations. It also involves the systematic monitoring of biometric equipment and systems to maintain operational security and ensure integrity of data and 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 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 implementation 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 <i>bold italicised</i> 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 Apply the principles of confidentiality, privacy and security in own work.	1.1 Applicable Occupational Health and Safety (OHS), legislative and organisational requirements relevant to the coordination of workplace biometric equipment and systems 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 Privacy and confidentiality of client data and information, verbal and written, is securely maintained in accordance with legislative and organisational requirements. 1.4 Potential confidentiality issues are promptly identified and clarified as required with relevant persons. 1.5 Effective communication and interpersonal techniques are used that reflect sensitivity to individual social and cultural differences.
2 Evaluate requirements for biometric equipment and systems.	2.1 Work order requirements are reviewed and verified in consultation with relevant persons. 2.2 Risk assessment information is reviewed and assessed for existing and potential threats or risks to organisational security. 2.3 Existing architecture is identified and assessed for effective integration with biometric equipment and systems. 2.4 Purpose, functions, modes and threshold levels of biometric equipment and systems are investigated and assessed against work order requirements. 2.5 Biometric equipment and systems are recommended, recorded and presented to relevant persons in accordance with workplace procedures.
3 Coordinate and implement processes.	3.1 Work schedules and roles and responsibilities are organised and allocated to relevant persons in accordance with workplace procedures. 3.2 Resources are organised and scheduled in accordance with workplace procedures. 3.3 Relevant administrative requirements are organised in accordance with legislative and organisational requirements. 3.4 Biometric equipment and systems are organised and located in accordance with work order requirements. 3.5 Required isolations of systems and networks and equipment are coordinated with relevant persons in

ELEMENT**PERFORMANCE CRITERIA**

	accordance with workplace procedures.
4 Maintain biometric equipment and systems and information.	4.1 Biometric equipment and systems are systematically and routinely monitored for optimum performance and ensure integrity of data and information. 4.2 Operational variations or non-conformance of biometric equipment and systems are identified and reported in accordance with workplace procedures. 4.3 Errors and deficiencies in data and information are identified and reported in accordance with workplace procedures. 4.4 Alternative options or recommendations for biometric equipment and systems to meet changing workplace needs and industry trends are reported in accordance with workplace procedures. 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 workplace biometric equipment and systems
- conduct a risk assessment and identify potential threats or risks to organisational security
- coordinate systems and networks and equipment isolations
- coordinate the implementation of biometric equipment and systems
- determine type and mode of biometric equipment and system to meet security requirements
- identify errors and deficiencies in received data and information
- identify operational variations or non-conformance of biometric equipment and systems
- make effective decisions
- organise work priorities and arrangements and complete work tasks within designated timeframes

REQUIRED SKILLS AND KNOWLEDGE

- 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
- 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 speaking clearly and questioning
- written communication skills sufficient to recommend and record biometric equipment and to complete 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 workplace biometric technology
- appropriate mathematical procedures for estimating, measuring and calculating
- biometric equipment and systems installation and implementation processes, procedures and requirements
- ergonomic and safe working practices and procedures
- established threshold levels and their impact on security
- information gathering techniques
- initial enrolment procedures
- operational principles of information technology
- organisational procedures for recording, reporting and maintaining workplace information
- organisational security plans, goals and objectives
- organisational standards, requirements, policies and procedures for the use of biometric technology
- performance testing methods
- principles of cultural diversity and access and equity
- privacy and ethics issues associated with biometric equipment and systems
- problem identification and resolution procedures
- project management tools and techniques
- security risk management processes and techniques
- threats, risks and hazards associated with biometric equipment and systems
- types, functions and parameters of biometric technology including software, hardware and acquisition devices
- 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:

- allocating roles and responsibilities, and organising schedules, resources, security authorisations, and isolations appropriate to implementing biometric equipment and systems
- 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
- determining requirements for biometric equipment and systems based on an accurate assessment of immediate security requirements
- evaluating operational effectiveness of integrating biometric equipment and systems with existing architecture
- maintaining operational security and ensuring integrity of data and information by the systematic monitoring of biometric equipment and systems
- recommending alternative options or recommendations of biometric equipment and systems to meet changing workplace needs and industry trends.

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 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.

Occupational Health and Safety (OHS) requirements may relate to:

- 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.

Legislative requirements may relate to:

- Australian standards and quality assurance requirements
- 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.

Biometric refers to:

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

Biometric equipment

- automated systems able to capture a biometric sample

and systems are: 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
- writing to audience needs.

Interpersonal techniques may involve:

- 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>Work order instructions and information may include:</i>	• access and authorisation requirements • OHS, confidentiality and other legal requirements • personal protection equipment • reporting and documentation requirements • resource and equipment requirements • risk and threat assessment assessments • security goals and objectives • work tasks and schedules.
<i>Threats:</i>	• are intentional or unintentional potential events that could compromise the security integrity of physical and technical organisational systems.
<i>Risks may relate to:</i>	• data and information • personnel • property.
<i>Existing architecture may include:</i>	• desktop PCs • local area networks (LANs) • mainframe systems • servers • websites • wide area networks (WANs).
<i>Mode may be:</i>	• multiple (a biometric system that integrates two ore more biometric technologies) • single.
<i>Resources may</i>	• biometric equipment and systems

- include:**
- equipment
 - human resources
 - tools.
- Administrative requirements may relate to:***
- access
 - authorisations
 - licensing.
- Records and reports:***
- may be:
 - computer-based
 - manual
 - other appropriate organisational communication system
 - may detail:
 - activity reports
 - allocated roles and responsibilities
 - biometric equipment and systems
 - errors in received data and information
 - operational faults and deficiencies
 - resource requirements
 - security requirements
 - technical data and specifications
 - work schedules.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Biometrics