



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC3024A Install biometric equipment and systems

Release: 1

CPPSEC3024A Install biometric equipment and systems

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to install a range of biometric equipment and systems in a security environment.

It requires the ability to read and interpret specifications, and use tools and equipment to effectively locate, install and commission biometric equipment and systems.

An understanding of the operating principles of biometric equipment, systems and technology is also required and well as the ability to 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 installation and operation of biometric equipment and systems. 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 the installation of <i>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 for installation.</p>	<p>2.1 <i>Work order</i> requirements are reviewed and confirmed as required with relevant persons.</p> <p>2.2 Relevant plans, drawings and specifications are accessed and interpreted against the work order.</p> <p>2.3 Biometric equipment and system to be installed is identified and confirmed against work order specifications.</p> <p>2.4 <i>Tools, equipment</i> and testing devices are selected appropriate to job requirement and checked for operational effectiveness in accordance with manufacturer's specifications.</p> <p>2.5 Licensing and site access requirements are identified and complied with.</p> <p>2.6 Coordination requirements, including requests for isolations, are requested and confirmed with relevant persons.</p> <p>2.7 Potential and existing risks and <i>hazards</i> in the work area are identified and controlled in accordance with OHS and organisational requirements.</p>
<p>3 Install biometric equipment and systems.</p>	<p>3.1 All work is conducted using safe operating procedures in accordance with OHS and organisational requirements.</p> <p>3.2 Biometric equipment and system is assembled, positioned and secured in accordance with relevant plans, drawings and specifications.</p> <p>3.3 Biometric equipment and system is installed in specified positions and locations in accordance with manufacturer's</p>

ELEMENT	PERFORMANCE CRITERIA
4 Complete installation.	<p>specifications.</p> <p>3.4 Biometric equipment and system is decommissioned and connected in accordance with manufacturer's specifications.</p> <p>3.5 Biometric equipment and system is installed without damage or distortion to the surrounding environment or services and in a manner that maximises safety of self and others.</p> <p>4.1 Basic operational testing of biometric equipment and system is conducted in accordance with manufacturer's specifications.</p> <p>4.2 Commission and test results confirm that biometric equipment and system is fully operational and meets installation performance specifications.</p> <p>4.3 Visual inspection of completed work is conducted to ensure installed biometric equipment and system complies with safety and environmental requirements.</p> <p>4.4 Faults, errors or omissions are identified and prompt remedial action is determined and arranged with relevant persons.</p> <p>4.5 Notification of completed installation is received and confirmed in accordance with workplace procedures.</p> <p>4.6 Records and reports are completed and maintained in accordance with legislative and organisational requirements.</p>

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 the installation of biometric equipment and systems
- install 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 appropriate information technology
- select and use appropriate tools and equipment, including hand and power tools
- use appropriate communication and interpersonal skills including speaking clearly and questioning
- 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 the full range of processes relating to the installation of biometric equipment and systems
- appropriate mathematical procedures for estimating, measuring and calculating
- cable identification and handling requirements
- earthing systems arrangements and requirements
- electrical concepts and connections
- ergonomic and safe working practices and procedures
- established threshold levels and their impact on security
- installation risks and hazards
- methods of installing biometric equipment and systems
- operational principles of information technology
- operational principles of local area networks (LANs) and wide area networks (WANs)
- organisational procedures for recording, reporting and maintaining workplace information
- organisational standards, requirements, policies and procedures for installing biometric equipment and systems
- physical environment requirements for the operation of biometric equipment and systems
- principles of cultural diversity and access and equity
- problem identification and resolution procedures
- types, functions and parameters of biometric equipment and systems
- 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 work tasks undertaken in the workplace
- conducting commissioning and visual inspections of installed biometric equipment and system to ensure installation conforms to required specifications
- organising relevant licensing and accessing authorisations relevant to undertaking the installation of biometric equipment and systems
- preparing for the installation of biometric equipment and system in the workplace including coordinating personnel and arranging required isolations
- selecting and using correct tools, equipment and testing devices and applying appropriate methods to safely position and installing biometric equipment and system.

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
 - Occupational Health and Safety (OHS)
- relevant industry codes of practice
- telecommunications.
- 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.
- data and information describes individual behavioural and physiological characteristics.
- 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

Organisational requirements may relate to:

Biometric:

Biometric equipment and systems are:

- 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.

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
- installation location
- licensing requirements
- OHS, confidentiality and other legal requirements
- personal protection equipment
- personnel coordination and isolation requirements
- reporting and documentation requirements
- resource and equipment requirements
- work tasks and schedules.

Tools and equipment may include:

- communications equipment
- hand tools
- multimeter
- personal protective equipment
- power tools
- testing equipment.

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).

Records and reports:

- may be:
 - computer-based
 - manual
 - other appropriate organisational communication system
- may detail:

- activity reports
- biometric equipment and systems installation
- commissioning details
- faults and repair requirements in processes
- technical data and specifications.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Biometrics