Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC3025A Identify and diagnose biometric system fault

Release: 1

CPPSEC3025A Identify and diagnose biometric system fault

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to conduct diagnostic testing of biometric systems to locate and verify faults.

It requires the ability to use and operate testing and diagnostic tools and equipment, collate data, and prepare reports based on an accurate assessment of test results and operational data.

An understanding of the basic operating principles, processes and parameters of biometric systems, together with applicable legislation including privacy requirements is also required.

This unit may form part of the licensing requirements for persons engaged in security operations involving biometric 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 use and diagnostic testing of biometric 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
1 Prepare for fault diagnosis.	1.1 Applicable ***Occupational Health and Safety*** (***OHS***), ***legislative*** and ***organisational requirements*** relevant to diagnosing faults in ***biometric 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 Work order is reviewed, confirmed and clarified as required with ***relevant persons***.
	1.4 ***Resources*** appropriate to work requirements are organised and checked for operational effectiveness in accordance with manufacturer's specifications.
	1.5 ***Information*** relevant to fault diagnosis activities is accessed and interpreted.
	1.6 Relevant authorisation for access to biometric system is arranged as required in accordance with workplace procedures.
	1.7 Requests for system isolation are coordinated and arranged with relevant persons in accordance with workplace procedures.
	1.8 Effective ***communication*** and ***interpersonal techniques*** are used that reflect sensitivity to individual ***social and cultural*** differences.
2 Diagnose faults.	2.1 Normal operational functions and performance of biometric system is confirmed and checked against specifications.
	2.2 System components are inspected for obvious faults and connections and cables checked for operation in accordance with manufacturer's specifications.
	2.3 ***Systematic fault-finding methods*** are used to identify and locate system fault.
	2.4 Appropriate diagnostic techniques are used to conduct tests of system in accordance with manufacturer's specifications.
	2.5 Test results are assessed against normal operational performance of system.
	2.6 Complex faults outside area of responsibility or competence are reported for specialist assistance.
3 Complete and report diagnosis.	3.1 Reports are prepared based on an assessment of diagnostic testing results and reviewed and checked for accuracy.
	3.2 Reports are prepared using ***appropriate formats*** and

ELEMENT	PERFORMANCE CRITERIA
	presentation methods in accordance with organisational requirements.
	3.3 Reports include valid and verifiable conclusions about the type and cause of identified system fault.
	3.4 Work area is reinstated to original condition and waste from work activities is collected, treated and disposed of in accordance with organisational requirements.
	3.5 ***Records and reports*** are completed and securely 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
- collate and record biometric data
- comply with applicable confidentiality and privacy requirements
- comply with legislation, regulations, standards, codes of practice relevant to the use and operation of a biometric system including privacy
- conduct checks for accurate and consistent information
- organise work priorities and arrangements and complete work tasks within designated timeframes
- read and interpret technical information including plans, designs and specifications
- read and interpret test results and data
- relate effectively to people from a range of social, cultural and ethnic backgrounds and varying physical and mental abilities
- resolve problems
- safely and correctly handle system components including connections and cables
- select and use testing tools and equipment and measurement instruments appropriate to work task
- undertake effective enrolment of biometric and biographical data
- use appropriate communication and interpersonal skills including speaking clearly and questioning
- verify and determine system faults
- written communication skills sufficient to develop a diagnosis report and complete other relevant records and reports.

REQUIRED SKILLS AND KNOWLEDGE

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 systems
- appropriate mathematical procedures for estimating, measuring and calculating
- biometric system administration and security requirements
- biometric system testing and diagnostic methods and techniques
- common biometric system performance problems
- data analysis techniques
- earthing systems arrangements and requirements
- electrical concepts (voltage, current, resistance and impedance)
- ergonomic and safe working practices and procedures
- established threshold levels and their impact on security
- initial enrolment procedures
- organisational procedures for recording, reporting and maintaining workplace information
- organisational standards, requirements, policies and procedures for the use, testing and operation of a biometric system
- principles of cultural diversity and access and equity
- problem identification and resolution procedures
- processes for the management of enrolment data
- system components and cabling handling requirements
- system fault-finding techniques
- types, functions and parameters of a biometric system
- types, functions and parameters of testing tools and equipment
- 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	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

competency in this unit

- complying with operational procedures for the use and testing of a biometric system including use of tools, equipment and measurement instruments
- complying with organisational policies and procedures, including OHS, relevant to biometric work tasks
- identifying and verifying faults in a biometric system and preparing data for presentation in a report
- reading, interpreting and assessing test results and biometric system data.

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 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 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 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.
***Resources* may include**:	• communications equipment • computer • hand tools • personal protective equipment and clothing • software and hardware • testing equipment (multimeter).
***Information* may include**:	• current system trending data • system configuration diagrams and installation records • system fault history • system specification schedules • system test data.
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.

Systematic fault-finding may involve:

- progressively isolating fault
- reviewing available data and information
- using a methodical approach
- verification of existence of problem.

Fault-finding methods may include:

- equipment program
- functionality tests
- visual inspection.

Appropriate formats may include:

- formats that cater for those with special needs for example, producing documents in large print.

Records and reports:

- may be:
  - computer-based
  - manual
  - other appropriate organisational communication system
- may detail:
  - activity reports
  - faults and diagnosis
  - operational details
  - technical data and specifications
  - testing and inspection results.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Biometrics