CPPSEC3022A Maintain biometrics database

Release: 1

CPPSEC3022A Maintain biometrics database

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit of competency specifies the outcomes required to maintain optimal performance of a biometrics database.
	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 and maintenance of biometric equipment and systems in a security environment. 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

Construction & Property Services Industry Skills Council

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 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 maintaining a ***biometric database*** is 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 Manage database security and access.	2.1 Database ***security and access*** arrangements are implemented and maintained in accordance with legislative and organisational requirements.
	2.2 Processes are implemented and monitored to ensure data and information is accessed by authorised personnel.
	2.3 Processes are established to monitor and maintain the quality and integrity of data and information retained on the database.
	2.4 Processes are established and maintained for the routine monitoring of the network server and ***computer system*** for security breaches.
	2.5 Procedures for the safe ***storage and protection*** of data and information are implemented and maintained.
3 Maintain database.	3.1 Biometric equipment and systems ***performance*** history is accessed and assessed and faults or breaches of security are promptly identified.
	3.2 Database is identified and relevant software and hardware installed as required in accordance with manufacturer's specifications.
	3.3 ***Relevant information*** regarding software and hardware maintenance is accessed and reviewed as required.
	3.4 ***Enrolment*** procedures are conducted in a systematic manner to ensure accuracy and currency of data.
	3.5 Virus protection is checked and updated as required to ensure continuous integrity and protection of data.
	3.6 Database ***backup*** procedures are appropriate for type and method of data storage and maintained in accordance with

ELEMENT	PERFORMANCE CRITERIA
	established housekeeping procedures.
4 Monitor database performance problems.	4.1 Operational performance-based biometric testing and reporting requirements are established and conducted in accordance with organisational requirements.
	4.2 *Performance problems* are identified and recorded.
	4.3 Appropriate database performance *diagnostic tool* is identified and used in accordance with manufacturer's specifications.
	4.4 Appropriate fixes are undertaken based on diagnostic results in consultation with appropriate personnel.
	4.5 Complex faults outside area of responsibility or competence are reported for specialist assistance.
5 Compile reports.	5.1 Results of maintenance operations are accurately and clearly recorded in accordance with workplace procedures.
	5.2 Maintenance operations are reviewed and procedures to *improve* effectiveness confirmed in consultation with appropriate personnel.
	5.3 Reports are prepared using *appropriate formats* and presentation methods in accordance with organisational requirements.
	5.4 Reports are produced based on gathered data and reviewed and checked for accuracy.
	5.5 *Records and reports* are 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
- apply best practice in backup and recovery strategies
- collate, interpret and record data
- comply with applicable confidentiality and privacy requirements
- comply with legislation, regulations, standards, codes of practice relevant to the use and operation of biometric technology and systems including databases

REQUIRED SKILLS AND KNOWLEDGE

- conduct checks for accurate and consistent information
- create simple queries using simple formulae
- facilitate effective change control mechanisms
- implement and maintain security of biometric technology and systems including databases
- 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
- resolve routine problems
- select and use appropriate information technology
- 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 performance problems, results of monitoring operations 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 the use and operation of biometric technology and systems including databases
- appropriate mathematical procedures for estimating, measuring and calculating
- backup and recovery methods
- common database performance problems
- data analysis techniques
- database administration, security and storage requirements
- database maintenance procedures
- ergonomic and safe working practices and procedures
- established threshold levels and their impact on security
- initial enrolment procedures
- management of enrolment data
- 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 maintaining a biometric database
- principles of cultural diversity and access and equity
- types and features of database design
- types, functions and parameters of a biometric database technology including

REQUIRED SKILLS AND KNOWLEDGE

    hardware and software including their application

- types, functions and parameters of diagnostic tools
- 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: • accurately documenting and maintaining operational reports • complying with applicable legislation and codes of ethics applicable to privacy and client confidentiality in maintaining biometric and biographical data • complying with organisational policies and procedures, including OHS, relevant to biometric work tasks • establishing processes to monitor and maintain user access and the secure management of a biometric database • identifying performance problems of a biometric database and carrying out appropriate fixes under relevant supervision • operational procedures and best practice standards for the maintenance of a biometric database and the secure storage of 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 equipment, systems and databases • access to plain English version of relevant statutes and procedures • assessment instruments including personal planner and assessment record book

Construction & Property Services Industry Skills Council

- 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

Construction & Property Services Industry Skills Council

- 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.

Construction & Property Services Industry Skills Council

Biometric refers to:	• a measurable physical characteristic or personal behavioural trait used to recognise the identity or verify the identity of an individual.
Biometric database includes:	• data describing individual behavioural and physiological characteristics.
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.

Construction & Property Services Industry Skills Council

***Social and cultural differences* may relate to**:	• dress and personal presentation • food • language • religion • social conventions • traditional practices • values and beliefs.
***Security and access* may relate to**:	• data inputting • search and browse authorities • viewing and operation • written permission.
Computer system may include:	• hardware and software components that run a computer.
***Storage and protection of data procedures* may include**:	• backups • security and authorised access requirements • storage in folders and sub-folders • storage on CD ROM, hard and floppy disk drives.
***Performance* may relate to**:	• compacting database files • improvements in response time • repairing the database • simultaneous access.
Relevant information may include:	• identification and supply of parts • schedule of maintenance • Standards (ISO, IEC, AS) • technical specialist activities • user recommended activities • version control.
***Enrolment* relates to**:	• the initial process of collecting biometric data from a user and storing it in a template for future comparison.
Backup:	• facilities may be a single tape unit or a more comprehensive, complex networked system • may include quality control and procedural information.
***Performance problems* may relate to**:	• failure to enrol rate (FTE or FER) • false accept rate (FAR) • false non match or reject rate (FRR).
***Diagnostic tools* may include**:	• electronics equipment (eg volt-meter, oscilloscope, data analyser) • software.
***Improvements* may relate to**:	• backup systems • changes to biometric settings • contingency plans

Construction & Property Services Industry Skills Council

	• threshold levels.
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: • faults and diagnosis • maintenance undertaken • operational details • recommended repairs • security breaches • testing and inspection results.

Unit Sector(s)

Unit sector   Security

Competency field

Competency field   Biometrics

Construction & Property Services Industry Skills Council