|  |  |
| --- | --- |
| **UNIT CODE** | CPPSEC3XXX |
| **UNIT TITLE** | Use and maintain security databases and compile reports |
| **APPLICATION** | This unit specifies the skills and knowledge required to use and maintain security databases and compile reports.It includes: * interpreting and complying with workplace procedures and policies, and with legal rights and responsibilities to set up hardware, software, databases and information systems to ensure continuous data integrity and protection, back-up and recovery
* using and maintaining security databases and a broad range of database functions to input, manipulate, store and retrieve verified data, check and rectify errors and variations in data quality, and diagnose and report processing errors and lags
* monitoring and reviewing database performance and effectiveness and using feedback to implement improvements
* compiling data in the required reporting format and checking data for accuracy, compatibility and reliability

It applies to people working independently or under limited supervision as members of a security team.This unit may form part of the licensing requirements for people engaged in security operations in those states and territories where these are regulated activities. |
| **PREREQUISITE UNIT** | Nil |
| **ELEMENTS** | **PERFORMANCE CRITERIA** |
| Elements describe the essential outcomes. | Performance criteria describe what needs to be done to demonstrate achievement of the element. |
| 1. Establish security database and systems. | 1.1 Interpret and comply with workplace procedures and policies and legal rights and responsibilities for maintaining and using security databases.1.2 Set up workstation to comply with ergonomic considerations and use work processes that conserve resources.1.3 Use software and hardware to meet data requirements following manufacturers’ specifications.1.4 Monitor and regularly update virus protection software to ensure continuous data integrity and protection.1.5 Confirm data access, security and storage requirements and set up systems to ensure data security and confidentiality.1.6 Set up and follow regular housekeeping, maintenance and back-up procedures.1.7 Implement stand-by database and alternative strategies to address operational faults and deficiencies in database systems. |
| 2. Use and maintain security database. | 2.1 Confirm and comply with data entry, output and presentation requirements to meet work instructions.2.2 Obtain data from verifiable sources and check for variations in data quality.2.3 Use database functions to input verified data, check data accuracy and quality, and rectify errors.2.4 Diagnose and report errors and lags in data processing or information discrepancies.2.5 Identify faults requiring specialist assistance and organise repairs in consultation with relevant persons.2.6 Monitor database performance and identify and implement measures to improve content, interfaces and effectiveness in consultation with relevant persons. |
| 3. Compile report and improve database and systems. | 3.1 Produce report in the required format, and check content to confirm accuracy and data compatibility and reliability.3.2 Request and use feedback to improve the effectiveness and performance of database and systems.3.3 Store and protect security data, and complete and maintain documentation with due regard to confidentiality. |
| ***FOUNDATION SKILLS***A person demonstrating competency in this unit must have the following language, literacy, numeracy and employment skills:* writing skills to:
	+ produce reports using information technology such as a computer and software
	+ collate and present data in a logical and sequential manner
* reading skills to interpret:
	+ procedures and policies that clarify legal rights and responsibilities
	+ manufacturers’ instructions to correctly set up hardware and database systems
	+ security data that may be technical and numerical in nature, such as database formulae and queries
* speaking and listening skills to:
	+ use questions and active listening to clarify and discuss system faults
	+ use paraphrasing to check understanding when receiving spoken feedback to improve systems
* numeracy skills to:
	+ interpret and calculate statistical information
	+ use simple mathematical formulae within databases
* problem solving skills to:
	+ verify the accuracy of security data
	+ recognise variations in data quality
	+ troubleshoot system problems and identify faults
* self-management skills to plan tasks to meet work timeframes
* technology skills to:
	+ use a range of common information technologies to access, store, study, retrieve, transmit and manipulate data and information, for example computer and software packages involving spreadsheets
	+ type and use a keyboard to enter data
 |
| **UNIT MAPPING INFORMATION** | Supersedes and is equivalent to CPPSEC3021A Maintain and use security database |
| **LINKS** | Companion volumes to this training package are available at the VETNet website:<https://vetnet.education.gov.au/Pages/TrainingDocs.aspx?q=6f3f9672-30e8-4835-b348-205dfcf13d9b> |

|  |  |
| --- | --- |
| **TITLE** | CPPSEC3XXX Use and maintain security databases and compile reports |
| **PERFORMANCE EVIDENCE** |
| A person who demonstrates competency in this unit must use and maintain security databases to compile reports to meet the requirements of two (2) different security assignments.In doing this, the person must meet the performance criteria for this unit. |
| **KNOWLEDGE EVIDENCE** |
| To be competent in this unit, a person must demonstrate knowledge of:* standard operating procedures and workplace policies that ensure compliance with legislative and regulatory requirements including:
	+ anti-discrimination and diversity
	+ duty of care
	+ limits of own authority
	+ privacy and surveillance
	+ workplace health and safety (WHS)
* backup and recovery methodologies used for security databases and systems
* basic research techniques that can be used to verify sources of security data
* data analysis techniques
* data entry procedures and processes
* database administration, security and storage requirements
* database functions and diagnostic tools
* methods for complying with privacy and confidentiality regulations when collecting, storing and disposing of security information
* methods for conserving energy and resources when using information technologies and their outputs
* methods for ensuring workstation meets ergonomic requirements
* presentation and reporting formats used for security data
* techniques for creating queries and formulae to analyse and process security data
* types of database software and hardware and their uses
 |
| **ASSESSMENT CONDITIONS**  |
| Assessors must satisfy the requirements for assessors contained in the Standards for Registered Training Organisations. Assessment of performance must be undertaken in an operational workplace environment or environment that reflects workplace conditions. Tasks are to be performed to the level of proficiency and within the time limits that would be expected in a workplace.Assessors are responsible for ensuring that the person demonstrating competency has access to:* specifications of assessment tasks to use and maintain security databases and compile reports
* appropriate documents, materials, equipment and personal protective equipment currently used in industry
* information technologies required to gather, organise and present security information and documentation
* standard operating procedures and workplace policies related to the security work role and which specify requirements for complying with industry legislation and regulations
 |
| **LINKS** | Companion volumes to this training package are available at the VETNet website:<https://vetnet.education.gov.au/Pages/TrainingDocs.aspx?q=6f3f9672-30e8-4835-b348-205dfcf13d9b> |

For inclusion in separate Companion Volume: Range Statements

|  |  |
| --- | --- |
| ***Workplace policies and legal rights and responsibilities*** may relate to: | * access and equity policies, principles and practices
* client service standards
* code of conduct and ethics
* communication and reporting procedures
* duty of care
* employer and employee rights and responsibilities
* own role, responsibilities and authority
* privacy and confidentiality of information
* professional standards, code of conduct and ethics
* resource parameters and procedures for accessing resources
* risk management
* storage and disposal of confidential information
* workplace health and safety (WHS) policies and procedures
 |
| ***Ergonomic considerations*** may include: | * avoiding radiation from computer screens
* chair height, seat and back adjustment
* document holder use
* footrest use
* lighting
* noise minimisation
* posture
* rest periods and exercise breaks
* screen, keyboard and mouse positions
* work station height and layout
 |
| ***Conserving resources*** may relate to**:**  | * recycling used and shredded paper
* using double-sided paper
* using re-used paper for drafts (observing confidentiality requirements)
* using power-save options for equipment
 |
| ***Access and security*** requirements may relate to: | * data inputting
* search and browse authorities
* viewing and operation
* write permission
 |
| ***Data entry, output and presentation*** requirements may relate to: | * author's instructions
* coding
* data input
* fault-finding
* installation or de-installation of software or hardware
* location and storage of data
* log-on
* password protection
* standard formats
* start-up or shutdown
* troubleshooting
* use of templates
 |
| ***Sources*** of data may include: | * computer data files
* government documents and registers
* media reports
* policy statements
* statistical summaries
* statutes
 |
| ***Checking*** data quality may relate to: | * accuracy of data
* accuracy of formulae
* consistency of data
* content
* filtering
* format
* proofreading
* spelling
 |
| ***Diagnosing*** errors may relate to: | * hardware
* input
* output
* running
* software
* troubleshooting procedures
 |
| ***Relevant persons*** may include: | * clients
* colleagues
* information storage specialists
* security personnel or consultants
* supervisors
 |
| Procedures for ***storing and protecting data*** may relate to: | * authorised access requirements
* backup
* maintaining hard or Cloud copies
* secure file locations
* storage (e.g. folders, sub-folders, hard drives, Cloud, server)
 |
| ***Feedback*** may include: | * comments from management, colleagues or clients
* formal and informal performance appraisals
* personal, reflective behaviour strategies
* workplace assessment
 |