



Australian Government

Department of Education, Employment and Workplace Relations

TLIK4008A Implement and monitor network security

Release: 1

TLIK4008A Implement and monitor network security

Modification History

Not Applicable

Unit Descriptor

Unit Descriptor

This unit involves the skills and knowledge required to implement and monitor network security. It involves identifying all security threats to the network and implementing approved controls to maintain network security integrity. This unit is derived from ICAITS123A Manage network security Licensing, legislative, regulatory or certification requirements are applicable to this unit.

Application of the Unit

Application of the Unit

Work may be undertaken in various contexts within the transport and distribution industry.

The unit generally applies to those who provide leadership of others individually or in teams.

This unit is normally packaged at AQF IV or above.

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. Assessment of performance is to be consistent with the evidence guide.

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
1 Identify threats	1.1 Implement risk analysis of security threats faced by organisation network 1.2 Evaluate and identify internal and external threats to network such as hackers, eavesdropping and viruses
2 Identify appropriate controls	2.1 Plans for cost effective improvements to network security are presented to management for approval and authorisation 2.2 External or intra network security devices and controls such as firewalls are presented to management for approval 2.3 Controls to add to the network to manage elements such as user access or hackers, eavesdropping and viruses are identified
3 Implement security	3.1 Approved equipment and controls are installed and configured to provide required levels of security 3.2 Recommendations are made for additional equipment and updates to maintain security integrity

Required Skills and Knowledge

REQUIRED KNOWLEDGE AND SKILLS

This describes the essential knowledge and skills and their level required for this unit.

Required knowledge:

- Relevant sections of national and state or territory regulatory requirements and codes of practice
- Current industry accepted hardware and software products with broad knowledge of general features and capabilities
- Broad general knowledge of the client business domain, business function and organisation
- Networking technologies, with broad knowledge of general features and capabilities incorporating substantial depth in some areas
- Risk analysis, with broad knowledge of general features incorporating substantial depth in some areas
- Specific security technology, with broad knowledge of general features incorporating substantial depth in some areas
- Procedures for operating electronic communications equipment
- Requirements for completing relevant documentation
- Code of practice for working collaboratively with others
- Typical defects that can occur and related action that should be taken

REQUIRED KNOWLEDGE AND SKILLS

- Procedures for identifying equipment defects and assessing for appropriate action
- Principles, purpose and location of controls, monitoring devices, and systems
- Steps involved in planning the work activities
- Procedures for adjusting controls to optimise the operation of the equipment
- Sources of information on differences in equipment and related standard operating and servicing procedures

Required skills:

- Use plain English literacy and communication skills in relation to analysis, evaluation and presentation of information
- Use questioning and active listening skills
- Read and interpret instructions, procedures, information and signs relevant to work activities
- Write reports for business requiring depth in some areas, analysis and evaluation of information in a defined range of areas
- Complete documentation related to work activities
- Operate electronic communication and other equipment to required protocol
- Work collaboratively with others
- Solve problems for a defined range of unpredictable problems involving participation in the development of strategic initiatives
- Use research to identify, analyse and evaluate broad features of a particular business domain and best practice in network security methodologies and technologies
- Project plan in relation to scope, time, cost, quality, communications and risk management
- Adapt appropriately to cultural differences in the workplace, including modes of behaviour and interactions with others
- Promptly report and/or rectify any identified problems, faults or malfunctions in accordance with regulatory requirements and workplace procedures
- Monitor work activities in terms of planned schedule
- Monitor performance of equipment

Evidence Guide

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required knowledge and skills, the range statement and the assessment guidelines for this Training Package.

EVIDENCE GUIDE

Critical aspects for assessment and evidence required to demonstrate competency in this unit

- The evidence required to demonstrate competency in this unit must be relevant to and satisfy all of the requirements of the elements and performance criteria of this unit and include demonstration of applying:
 - the underpinning knowledge and skills
 - relevant legislation and workplace procedures
 - other relevant aspects of the range statement

Context of and specific resources for assessment

- Performance is demonstrated consistently over a period of time and in a suitable range of contexts
- Resources for assessment include:
 - a range of relevant exercises, case studies and/or other simulated practical and knowledge assessment, and/or
 - access to an appropriate range of relevant operational situations in the workplace
- In both real and simulated environments, access is required to:
 - relevant and appropriate materials and equipment, and
 - applicable documentation including workplace procedures, regulations, codes of practice and operation manuals

Method of assessment

- Assessment of this unit must be undertaken by a registered training organisation
- As a minimum, assessment of knowledge must be conducted through appropriate written/oral tests
- Practical assessment must occur:
 - through activities in an appropriately simulated environment at the registered training organisation, and/or
 - in an appropriate range of situations in the workplace

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.

Software most likely to be:

- packaged software

RANGE STATEMENT

Depending on the organisation concerned, workplace procedures may be called:	• supplied from many varying vendors • security, audit, virus checking and encryption modules • standard operating procedures (SOPs) • company procedures • enterprise procedures • organisational procedures • established procedures
Communication in the work area may include:	• phone • electronic data interchange (EDI) • fax • email • internet • intranet • RF systems • oral, aural or signed communications
Consultative processes may involve:	• other employees and supervisors • suppliers of network security equipment • relevant authorities and institutions • management
Documentation and records may include:	• quality assurance procedures • emergency procedures • operations manuals • manufacturers specifications for network equipment • technical instructions • relevant Australian Standards and certification requirements

Unit Sector(s)

Not Applicable

Competency Field

Competency Field K - Technology