Australian Government

Department of Education, Employment and Workplace Relations

ICANWK301A Provide network systems administration

Release: 1

ICANWK301A Provide network systems administration

Modification History

Release	Comments
Release 1	This Unit first released with *ICA11 Information and Communications Technology Training Package version 1.0*

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to technically manage elements of a network, including contributing to disaster recovery plan.

Application of the Unit

This unit applies to frontline technical support personnel responsible for administering a network.

Licensing/Regulatory Information

No licensing, legislative, regulatory or certification requirements apply to this unit at the time of endorsement but users should confirm requirements with the relevant federal, state or territory authority.

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Element	Performance Criteria
Elements describe the essential outcomes of a unit of competency.	*Performance criteria describe the 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 the range statement. Assessment of performance is to be consistent with the evidence guide.*

Elements and Performance Criteria

1. Provide client access and security	1.1 Provide logons, passwords and applications file access to ***users*** and prepare ***documentation*** in line with ***organisational requirements*** 1.2 Examine records of user accounts to determine access privileges and usage 1.3 Take necessary action to ensure maintenance of ***system*** integrity and security
2. Provide input into and disseminate disaster recovery plan	2.1 Provide input into the organisation's ***disaster recovery plan*** 2.2 Disseminate disaster recovery plan to users as required
3. Monitor network performance	3.1 Perform diagnostic tests associated with administering the network or system 3.2 Analyse and respond to diagnostic information 3.3 Monitor ***software*** usage, including inappropriate or illegal use 3.4 Delete illegal software from the system 3.5 Monitor ***hardware*** response time and other performance indicators 3.6 Determine and action methods for improving network and systems efficiency according to ***organisational guidelines***

Required Skills and Knowledge

This section describes the skills and knowledge required for this unit.

Required skills

- communication skills to:
  - investigate and assess client needs
  - provide one-to-one instruction
- customer-service skills to communicate with clients in a range of contexts at various levels
- literacy skills to:
  - develop reports
  - interpret technical manuals
- planning and organisational skills to provide input into the disaster recovery plan
- technical skills to perform:
  - diagnostic tests to monitor network performance
  - system administration tasks.

Required knowledge

- advanced knowledge of software features supported by the organisation
- approaches to backup and restoring computer data
- disaster recovery policy
- features and functions of file access
- in-house and vendor support
- OHS legislation relating to the use of equipment
- operating systems:
  - functions and basic features
  - supported by the organisation
- organisational access and security procedures
- organisational and technical systems
- organisational procedures for protection against and elimination of computer viruses
- policy and procedures for deleting, restoring and archiving files
- procedures for creating logons
- security and network guidelines and procedures
- software copyright responsibilities.

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.

Overview of assessment	
Critical aspects for assessment and evidence required to demonstrate competency in this unit	Evidence of the ability to: • sustain the operation of the network through maintenance of network integrity and perform diagnostic tests • contribute to the formulation of a disaster recovery plan and provide the client with an optimised network that complies with organisational guidelines • improve network and systems efficiency according to organisational guidelines • provide appropriate access to the network for users • maintain, limit or enhance user access according to authorised requests.
Context of and specific resources for assessment	Assessment must ensure access to: • live network • systems administration tools currently used in industry • organisational policy and procedures • appropriate learning and assessment support when required • modified equipment for people with special needs.

Method of assessment	A range of assessment methods should be used to assess practical skills and knowledge. The following examples are appropriate for this unit:
	• review of documentation completed by candidate for provision of client access and security
	• documented input into disaster recovery plan
	• direct observation of candidate:
	  • performing diagnostic tests and responding to diagnostic information
	  • performing user maintenance tasks
	• verbal or written questioning to assess candidate's knowledge of methods for improving network and systems efficiency.

Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, where appropriate. Assessment processes and techniques must be culturally appropriate, and suitable to the communication skill level,

	language, literacy and numeracy capacity of the candidate and the work being performed. Indigenous people and other people from a non-English speaking background may need additional support. In cases where practical assessment is used it should be combined with targeted questioning to assess required knowledge.

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.

Users may include:	• contractors • departments within an organisation • persons within a department • support staff • third parties.
Documentation may follow:	• audit trails • client training • equipment inventory maintenance • International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and Australian Standards (AS) standards • naming standards • project-management templates and report writing • satisfaction reports • version control.
Organisational requirements may be in reference to:	• diagnostic policy • preventative maintenance • problem solution processes • roles and technical responsibilities in the IT department • vendor and product service level support agreements • work environment.
System may include:	• application • business • computers • financial system • information system • management system • network • software.
Disaster recovery plan may include:	• backup plans • disaster recovery activities • impact assessment • key roles and responsibilities • maximum tolerable outage

	• recovery time • risk analysis • zero data loss.

Software may include:	• application:
	  • database
	  • internet browser
	  • spreadsheet
	  • word-processing
	• commercial
	• customised
	• in-house
	• programming:
	  • assembler
	  • compiler
	  • development tools
	• system:
	  • computer security
	  • device drivers
	  • operating system.

Hardware may include:	• modems or other connectivity devices • networks • personal computers • remote sites • servers • workstations.
Organisational guidelines may include:	• communication methods • content of emails • dispute resolution • document procedures and templates • downloading information and accessing particular websites • financial control mechanisms • opening mail with attachments • personal use of emails and internet access • virus risk.

Unit Sector(s)

Networking