



Australian Government

Department of Education, Employment and Workplace Relations

ICASAS304A Provide basic system administration

Release: 1

ICASAS304A Provide basic system administration

Modification History

Version	Comments
ICASAS304A	This version first released with <i>ICA11 Information and Communications Technology Training Package version 1.0</i>

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to implement components of systems backup, restore, security and licensing in a stand-alone or client server environment.

Application of the Unit

Frontline technical support personnel apply the skills and knowledge in this unit, and generally work under limited supervision with experienced IT support staff. Support personnel at this level use known routines and procedures where some discretion and judgement are required, and provide technical advice and some leadership in resolution of specified problems. More complex or non-routine activities involving individual responsibility may be performed as part of a group or team and the role may involve some responsibility for others.

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
<i>Elements describe the essential outcomes of a unit of competency.</i>	<i>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.</i>

Elements and Performance Criteria

1. Record security access	1.1 Obtain client access requirements and clearance levels according to organisational requirements 1.2 Issue computer or network user account and password details to client 1.3 Provide security documentation and access to client 1.4 Record user account and security access details to maintain system integrity and assist later auditing
2. Record software licences	2.1 Determine what licensed software is used within the organisation 2.2 Maintain records of licence number and location 2.3 Check personal computers and network for illegal software 2.3 Report illegal software to appropriate person
3. Carry out system backup	3.1 Create or review organisational backup schedule 3.2 Complete file backups according to schedule 3.3 Label and store backups according to organisational requirements 3.4 Maintain record of backups
4. Restore system backup	4.1 Determine and test restore procedures according to organisational guidelines 4.2 Complete a restore under supervision of an appropriate person 4.3 Record completed restore according to organisational guidelines
5. Apply security access controls	5.1 Document security access as per clearance guidelines set by management 5.2 Maintain a security access register in line with organisational guidelines to record which client or groups have access to which resources 5.3 Identify the security controls on the file system provided by the operating system 5.4 Apply effective access control on files and directories

Required Skills and Knowledge

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

Required skills

- literacy skills to:
 - interpret user manuals, technical documentation and help functions
 - maintain inventory records
 - record software licence records
- communication skills to:
 - communicate with peers and supervisors
 - present and explain information
 - seek assistance and expert advice
- planning and organisational skills to plan and develop a backup and restore strategy
- technical skills to:
 - configure user account and security access details
 - identify unlicensed software
 - record user account and security access details.

Required knowledge

- backup procedures
- operating systems used by the organisation
- organisational security procedures
- organisational standards to:
 - carry out backup and restore operations
 - label and store backups
- selection, functions and features of appropriate diagnostic tools
- software copyright responsibilities
- system's current functionality.

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: - perform systems backup, restore and maintain correct usage according to licensing agreements in a stand-alone or client server environment - maintain software licence records and check for copyright compliance within the system - maintain security access details in a register and apply access controls on (network) resources.
Context of and specific resources for assessment	Assessment must ensure access to: - sites with a representative range of stand-alone and networked client-server environments and operating systems - software licence records - technical records and documentation - organisational backup and restore procedures - organisational security guidelines - 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: - direct observation of candidate undertaking file backup and restoration - review of records on backup results and backup schedules - review of software licence records - review of the event viewer - verbal or written questioning to assess candidate's knowledge of software copyright compliance.
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.

<i>Client</i> may include:	• employee • external organisation • individual • internal department.
<i>Organisational requirements</i> may include:	• availability of system to be optimised • client-support documentation • complexity of technical manuals • information and communications technology (ICT) policy and procedures relating to service levels and installation • in-house or vendor ICT purchasing arrangements • register of licences • security procedures • storage of ICT documentation • system administration and backup procedures • type of product licences.
<i>Documentation</i> may follow:	• audit trails • client training • International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and Australian Standards (AS) standards • maintaining equipment inventory • naming standards • project-management templates and report writing • satisfaction reports • version control.
<i>Software</i> may include:	• application: • database • internet browser • spreadsheet • word-processing • commercial applications • customised • in-house

	• programming: • assembler • Java, VB, C++, Visual Fox Pro • compiler • development tools • system: • computer security • operating system.
Records may include:	• databases • spreadsheets • vendor tools to create, modify and document user accounts • access to computer or network resources.
Appropriate person may include:	• authorised business representative • client • supervisor • system administrator.
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.
Operating systems may include:	• GNU and Linux • Mac OS X • Microsoft Windows • Unix-like operating systems: • HP-UX • IBM AIX • Silicon Graphics IRIX • Sun Solaris.

Unit Sector(s)

Systems administration and support

