Australian Government

Department of Education, Employment and Workplace Relations

ICASAS207A Protect and secure information assets

Release: 1

ICASAS207A Protect and secure information assets

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 ensure information assets are protected from improper access and appropriate actions are taken to secure assets in the event that they are threatened.

Application of the Unit

This unit applies to technical support personnel who are required to protect and secure equipment in a small or large office environment. Maintaining asset security and implementing preventive security measures are key components of any information and communications technology (ICT) environment.

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. Identify assets and threats	1.1 Identify types of ***information assets*** in the ***organisation*** 1.2 Identify mechanisms by which information assets are accessed, transmitted and stored 1.3 Establish nature of threats to information assets and determine ***effect*** that ***loss or damage*** may have to the organisation
2. Secure assets	2.1 Identify actions, mechanisms and strategies to protect information assets 2.2 ***Secure*** assets within scope of authority 2.3 Report issues to ***appropriate person*** and other issues where they are outside scope of authority
3. Mitigate or prevent damage to assets	3.1 Identify signs and evidence that information assets are threatened or undergoing loss or damage 3.2 Provide ***first-level response*** to reduce affects, mitigate damage and protect evidence 3.3 Report incident, effects and actions to appropriate person

Required Skills and Knowledge

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

Required skills

- literacy and communication skills to:
  - present information
  - report incidents where assets are threatened
- problem-solving skills to:
  - anticipate and respond to threats to information assets
  - solve known problems in routine procedures
- technical skills to:
  - install and activate system filtering and security settings
  - operate a computer and software application
  - protect and secure information assets
  - provide first-level response.

Required knowledge

- information assets and key sources of information assets
- types of security options available to secure assets
- assets supported by the organisation
- general ICT hardware
- organisation's security procedures.

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: • conduct an audit of information assets, the potential threats and effect on the organisation • identify threats to assets and take appropriate action to overcome them • communicate and discuss details of security threats and issues relating to information assets.
Context of and specific resources for assessment	Assessment must ensure access to: • sites with computer hardware and office environments representing a range of workplaces • a range of appropriate software systems • organisational information assets • technical records, documentation and enterprise procedures • appropriate learning and assessment support when required. Where applicable, physical resources should include equipment modified 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 conducting an audit of information assets • review of audit records prepared verbal or written questioning to assess candidate's knowledge of nature of threats and effect of threats • review of reports, including examples of different threats and associated actions.
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.

Information assets may include:	• equipment • files • forms • online or printed data and information • passkeys or passwords • procedures • programs or information channels • reports.
Organisation may include:	• departments • entities outside the business • government • individuals inside and outside the business • the whole business.
Affect may include:	• confidentiality • financial • personal • privacy issues • reputation.
Loss or damage may include:	• alteration • damage or destruction • deletion • misuse • theft • unauthorised publication.
Secure may include:	• appropriate modification of procedures or processes • changing of passwords or work habits • physical exclusion or control • protective software installation or operation.
Appropriate person may include:	• business owner or authorised business representative • client • government • peers • police as appropriate

	• supervisor.
First-level response may include:	• changing passwords • excluding people from access • locking doors • locking down the workplace • logging off • powering down systems • updating software protection.

Unit Sector(s)

Systems administration and support