



Australian Government

ICTSAS207 Protect and secure information assets

Release: 1

ICTSAS207 Protect and secure information assets

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 1.0.

Application

This unit describes the 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.

It applies to individuals who, while working under a level of supervision, have responsibility in a frontline technical support capacity to exercise in a small or large office environment.

No licensing, legislative or certification requirements apply to this unit at the time of publication.

Unit Sector

Systems administration and support

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
<i>Elements describe the essential outcomes.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element.</i>
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

ELEMENT	PERFORMANCE CRITERIA
	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 effects, mitigate damage and protect evidence 3.3 Report incident, effects and actions to appropriate person

Foundation Skills

This section describes language, literacy, numeracy and employment skills incorporated in the performance criteria that are required for competent performance.

Skill	Performance Criteria	Description
Reading	1.1-1.3, 2.2, 2.3, 3.1	Researches and interprets text to identify misleading information and compare technical specifications, and identify solutions to new and emerging issues to maintain system
Writing	2.3, 3.3	Uses simple vocabulary to report textual information in a sequential manner to the appropriate personnel
Oral Communication	2.3	Presents factual information in a clear manner, using specific and appropriate language
Navigate the world of work	1.1-1.3, 2.1-2.3, 3.1-3.3	Understands roles and responsibilities for task and makes basic decisions on work completion parameters in accordance with organisational standards
Interact with others	2.2, 2.3	Identifies and takes steps to follow accepted communication practices and protocols
Get the work done	1.1-1.3, 2.1-2.3, 3.1-3.3	- Plans and implements routine tasks, aiming to achieve them efficiently - Initiates standard diagnostic procedures when responding to familiar and unfamiliar problems within immediate context, and seeks input from others when problems remain unresolved - Understands the purposes, specific functions and key features of common digital systems and tools, and operates them effectively to complete routine tasks

Unit Mapping Information

Code and title current version	Code and title previous version	Comments	Equivalence status
ICTSAS207 Protect and secure information assets	ICASAS207A Protect and secure information assets	Updated to meet Standards for Training Packages	Equivalent unit

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>

Assessment Requirements for ICTSAS207 Protect and secure information assets

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 1.0.

Performance Evidence

Evidence of the ability to:

- identify the organisation's information assets and the ways in which these assets are used
- establish potential threats to information assets and analyse the effects these threats would have on the organisation
- implement measures to secure assets, and mitigate or prevent damage, according to organisational requirements
- discuss details of security threats and issues relating to information assets with appropriate persons
- report issues or incidents according to organisational requirements.

Note: If a specific volume or frequency is not stated, then evidence must be provided at least once.

Knowledge Evidence

To complete the unit requirements safely and effectively, the individual must:

- identify information assets and key sources of information assets
- identify the types of security responses available to secure assets
- identify assets supported by the organisation
- describe general information and communications technology (ICT) hardware and security implications
- identify the organisation's security procedures.

Assessment Conditions

Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the systems administration and support field of work and include access to:

- a site with computer hardware and office environments representing a range of workplaces
- appropriate software systems
- organisational information assets
- technical records, documentation and enterprise procedures.

Assessors must satisfy NVR/AQTF assessor requirements.

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>