Australian Government

Department of Education, Employment and Workplace Relations

ICAS2248A Protect and secure information assets

Release: 1

ICAS2248A Protect and secure information assets

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required for ensuring information assets are protected from improper access and appropriate actions are taken to secure assets in the event that they are threatened. *No licensing, legislative, regulatory or certification requirements apply to this unit at the time of publication.*

Application of the Unit

Application of the unit	

Licensing/Regulatory Information

Refer to Unit Descriptor

Pre-Requisites

Prerequisite units		
	ICAU2231B	Use a computer operating system

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 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

ELEMENT	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 the ***impact*** that ***loss or damage*** may have to the organisation
2. Secure assets	2.1. Identify the actions, mechanisms and strategies to protect information assets 2.2. ***Secure*** assets within scope of authority and report these issues ***to appropriate person*** and other issues where it is 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 impacts, mitigate damage and protect evidence 3.3. Report incident, effects and actions to appropriate person

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Basic knowledge of Information assets
- Broad general knowledge of operating systems supported by the organisation
- Broad general knowledge of computer hardware
- Basic knowledge types protective applications used against viruses and spam and other threats
- Interaction between relevant hardware and software products and communication devices
- Broad knowledge of the client business domain

Required knowledge

- Identification of key sources of information assets
- Decision making in a limited range of options

REQUIRED SKILLS AND KNOWLEDGE
• Problem solving of known problems in routine procedures • Plain English literacy and communication skills in relation to the presentation of information • Basic skills in computer operation and software application operation • Ability to install and/or activate system filtering and security settings

Evidence Guide

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 following is essential: • Assessment must confirm the ability to conduct research and discuss various security issues relating to Information assets. • Assessment must confirm the ability to examine and discuss examples of different actions using case studies
Context of and specific resources for assessment	Threats to information assets is ever present and an appropriate understanding of how these assets should be protected and the response and actions in the event of an attack, loss or damaging event is important for every individual in the workplace. The breadth, depth and complexity of knowledge and skills in this competency would prepare a person to perform in a range of varied activities or knowledge applications where there is a clearly defined range of contexts in which the choice of actions required is usually clear. There would generally be limited complexity in the range of operations to be applied. Performance of a prescribed range of functions involving known routines and procedures and some accountability for the quality of outcomes would be characteristic. Applications may include some complex or non-routine activities involving individual responsibility or autonomy and/or collaboration with others as part of a group or team. To demonstrate this unit of competency the learner will require access to: • The organisation's applications needs and

EVIDENCE GUIDE	
	information types • Appropriate software systems • Computer hardware and office environments representative of a range of workplaces
Method of assessment	The purpose of this unit is to define the standard of performance to be achieved in the workplace. In undertaking training and assessment activities related to this unit, consideration should be given to the implementation of appropriate diversity and accessibility practices in order to accommodate people who may have special needs. Additional guidance on these and related matters is provided in ICA05 Section 1. The following assessment method is appropriate for this unit: • Assessment of this unit of Competency will usually include observation of real or simulated work processes and procedures, quality projects, questioning on underpinning knowledge and skills. This competency can be assessed in the workplace or in a simulated environment. Simulated activities must closely reflect the workplace to fully demonstrate Competency. • Competency in this unit needs to be assessed using summative assessment to ensure consistency of performance in a range of contexts.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended. An individual demonstrating this competency would be able to: • Demonstrate basic operational knowledge in a moderate range of areas • Apply a defined range of skills • Apply known solutions to a limited range of

EVIDENCE GUIDE	
	predictable problems • Perform a range of tasks where choice between a limited range of options is required • Assess and record information from varied sources • Take limited responsibility for own outputs in work and learning • Maintain knowledge of industry products and services

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. 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:	• forms • procedures • reports • files • online or printed data and information • passkeys or passwords • programs or information channels • equipment
Organisation may include:	• individuals inside and outside the business • departments • the whole business • entities outside the business • government
Impact may include:	• financial • personal • reputation • privacy issues • confidentiality
Loss or damage may include:	• theft • damage or destruction

RANGE STATEMENT	
	• unauthorised publication • deletion • alteration • misuse
Secure may include:	• protective software installation or operation • appropriate modification of procedures or processes • changing of passwords or work habits • physical exclusion or control, etc.
Appropriate person may include:	• supervisor • peers • business owner or authorised business representative • government • client • police as appropriate
First level response may include:	• updating software protection • logging off • powering down systems • changing passwords • locking doors • excluding people from access • locking down the workplace

Unit Sector(s)

Unit sector	Support

Co-requisite units

Co-requisite units		

Competency field

Competency field	