



Australian Government

ICTCYS402 Identify and confirm cyber security incidents

Release: 1

ICTCYS402 Identify and confirm cyber security incidents

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 6.0.

Application

This unit describes the skills and knowledge required to identify, confirm and report cyber security incidents in an organisation.

It applies to individuals who work in information technology security, and gather logs from systems, networks and applications to identify the occurrence of incidents in any business environment.

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

Unit Sector

Cyber security

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 cyber security incidents	1.1 Identify and review legislative requirements and organisational procedures and policies applicable to cyber security incidents and incident response plans 1.2 Obtain and analyse system, network and application infrastructure and logs according to organisational security procedures 1.3 Analyse and test application and confirm assumptions of incidents according to organisational security procedures 1.4 Discuss differences between network and systems incidents with required personnel
2. Confirm cyber security incidents	2.1 Confirm whether incidents are network or systems related 2.2 Discuss and confirm incident with required personnel

ELEMENT	PERFORMANCE CRITERIA
	2.3 Identify and discuss potential changes required to system, network and application
3. Report and document cyber security incidents	3.1 Report cyber security incident to required personnel, according to legislative requirements and organisational policies and procedures 3.2 Document exposed vulnerability and changes, solutions and actions discussed according to organisational policies and procedures

Foundation Skills

This section describes those language, literacy, numeracy and employment skills that are essential to performance but not explicit in the performance criteria.

SKILL	DESCRIPTION
Learning	Identifies and gathers information applicable to business, systems, network and infrastructure
Oral communication	Uses effective communication techniques to discuss details of cyber security incidents using industry standard technical language intended for audience and environment
Reading	- Interprets information in a range of formats when identifying cyber security incidents - Reads and applies information of relevance to cyber security incident and suggests potential changes
Writing	Uses required and industry specific terminology in documenting cyber security incidents and proposed actions and solutions
Technology	Uses required technological tools and software in identifying and confirming cyber security incidents

Unit Mapping Information

No equivalent unit. New unit.

Links

Companion Volume Implementation Guide is found on VETNet -

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