Australian Government

ICTCYS406 Respond to cyber security incidents

Release: 2

ICTCYS406 Respond to cyber security incidents

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 6.0.
Release 2	Correcting an error in the Knowledge Evidence.

Application

This unit describes the skills and knowledge required to establish and respond to cyber security incidents in an organisation, and evaluate actions performed to mitigate risk of future incidents.

It applies to individuals who work in information technology security, including network specialists and security, to support all business functions responding to cyber incidents. These individuals have a broad range of knowledge and skills in cyber security, networks and systems. In this context, the individual works as an internal function for an organisation, however, the same can be applied in the context of an external security specialist advising and implementing the response and action items of a cyber-attack to an external client.

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
Elements describe the essential outcomes.	*Performance criteria describe the performance needed to demonstrate achievement of the element.*
1. Establish cyber security incident	1.1 Establish and confirm occurrence and nature of cyber security incident 1.2 Identify legislative requirements, organisational policies and procedures and cyber security incident response plans 1.3 Analyse and assess source, impact and consequences of incident according to organisational response plans 1.4 Notify and explain cyber incident to required personnel

ELEMENT	PERFORMANCE CRITERIA
	according to legislative requirements and communications plans
2. Activate cyber security incident response plan	2.1 Activate incident response plan and confirm cyber incident is contained 2.2 Escalate and involve third party services and specialists as required according to organisational policies and procedures 2.3 Confirm no further risks exist according to legislative requirements and organisational response procedures 2.4 Discuss solutions with required personnel and action accordingly 2.5 Test solution implemented, and escalate as required according to organisational security procedures
3. Perform post cyber security incident response procedures	3.1 Evaluate actions taken and confirm incident is fixed and secure according to organisational procedures 3.2 Document cyber security incident, actions performed and solution, according to organisational policies and procedures 3.3 Discuss and document lessons learnt with required personnel 3.4 Discuss and implement preventative measures and mitigation methods as required 3.5 Amend incident response plan accordingly 3.6 Share documentation and communicate with required personnel according to organisational communications plan

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 organisational procedures and incident response procedures
Numeracy	• Measures and records mathematical data and uses tools when interpreting results
Reading	• Identifies and interprets information from incident response plans, and extracts applicable areas when dealing with cyber security incidents

SKILL	DESCRIPTION
Writing	• Uses required industry specific terminology when documenting cyber security incidents and solutions
Problem solving	• Uses problem solving skills when identifying the nature and impact of cyber security incidents
Technology	• Uses required technological tools and software in responding to cyber security incidents • Applies skills in systems administration, network security, applications and programming

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