



Australian Government

ICTCYS405 Develop cyber security incident response plans

Release: 1

ICTCYS405 Develop cyber security incident response plans

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 plan for and develop a response plan for cyber security incidents.

It applies to individuals who work in information technology security, including network and security specialists, and apply a range of cyber security threat skills and knowledge to support all business functions plans for incidents.

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. Plan incident response plans	1.1 Identify and gather information on organisational environment, procedures and processes and cyber security threats 1.2 Discuss and confirm ideas and plans with management and gain approval in developing response plans 1.3 Establish response committee and roles and responsibilities of each individual according to organisational procedures 1.4 Identify required services and assets in developing test plans
2. Develop and confirm incident response plans	2.1 Establish and confirm recovery time objective (RTO) and recovery point objective (RPO) in disaster recovery according to organisational requirements 2.2 Discuss and establish test scenarios 2.3 Establish and confirm test frequency according to

ELEMENT	PERFORMANCE CRITERIA
	organisational requirements 2.4 Develop test baselines and metrics according to organisational procedures 2.5 Confirm and document draft test plans with required personnel and respond to feedback accordingly 2.6 Test cyber security incident response plan according to testing procedures 2.7 Identify, address and report errors noted in testing phase, within scope of own role
3. Finalise incident response plans	3.1 Discuss lessons learnt in testing response plans and adjust test plans accordingly 3.2 Obtain sign-off with required personnel according to organisational policies and procedures 3.3 Record, document and store test plans according to organisational 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 organisational procedures and developing response plans
Numeracy	Uses tools to measure and record data and interpret test plan results
Reading	Identifies and analyses information from a broad range of sources in determining required incident response plans suited to an organisation
Writing	Prepares complex workplace documentation detailing response plans using required structure, layout and technical programming language
Technology	Uses required technology tools and software in testing cyber security response plans

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>

Assessment Requirements for ICTCYS405 Develop cyber security incident response plans

Modification History

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

Performance Evidence

The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to:

- develop a plan in response to cyber security incidents for each of the following areas:
 - organisation's network
 - organisation's system
 - Wi-Fi network
 - an application
 - a human error.

In the course of the above, the candidate must:

- establish at least two test scenarios in each plan
- develop at least two test metrics and at least two baselines in each plan
- adhere to organisational procedures.

Knowledge Evidence

The candidate must be able to demonstrate knowledge to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including knowledge of:

- features and principals of networking, Wi-Fi networks and applications
- procedures in testing cyber security incident test plans
- metrics and baselines used in cyber security incident test plans
- roles and responsibilities of test committees
- organisational procedures and requirements applicable to developing cyber security incident response plans, including:
 - documenting established requirements and incident response plans
 - establishing response committees
 - testing methodologies

- establishing baselines and metrics
- cyber incidents and scenarios.

Assessment Conditions

Skills in this unit must be demonstrated in a workplace or simulated environment where the conditions are typical of those in a working environment in this industry.

This includes access to:

- software required in testing cyber security incident response plans
- required hardware and its components
- Wi-Fi network
- an application
- text-editing software
- information applicable to organisational environment, processes and previous cyber security incidents.

Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

Links

Companion Volume Implementation Guide is found on VETNet -

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