



Australian Government

Assessment Requirements for ICTCYS406 Respond to cyber security incidents

Release: 2

Assessment Requirements for 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.

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:

- respond to at least two different cyber security incidents in at least two different business functions
- develop and follow a basic communications plan.

In the course of the above, the candidate must:

- comply with organisational cyber security incident response plan
- adhere to legislative requirements and organisational policies and 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:

- key features of incident response plans
- cyber security incidents and the source and causes of these incidents
- types of attacks, including:
 - denial-of-service attack (DoS)
 - SQL injection (SQLi)
 - cross-site scripting (XSS) attacks
 - scripted attacks
 - hardware attacks
 - attacks against Wi Fi
- cyber security incident detection methodologies
- preventative measures and mitigation methods applicable to cyber security incidents

- documentation processes that may be used in the process of responding to cyber security incidents
- organisational policies and procedures applicable to cyber security incident response, including procedures for:
 - determining nature and location of incidents
 - containing incidents, including installation of security patches and disabling network access
 - notifying and reporting to required personnel
 - encryptions
 - assessing impact on business function and other areas
- procedures in developing communications plans.

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:

- organisation cyber security incident response plan
- required hardware and software
- text-editing software
- legislative requirements and organisational procedures and policies applicable to cyber security incident.

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>