Australian Government

Assessment Requirements for ICTCYS402 Identify and confirm cyber security incidents

Release: 1

Assessment Requirements for 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.

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:

- identify and confirm occurrence of at least:
  - one network incident
  - one system incident
  - one wireless or Wi-Fi incident
  - one application incident.

In the course of the above, the candidate must:

- discuss and contribute at least one potential change to each incident
- adhere to legislative requirements and organisational security 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:

- different types of cyber security incidents and attacks, including:
  - security vulnerabilities and malware
  - denial-of-service attack (DDOS)
  - SQL injection (SQLi)
  - cross-site scripting (XSS) attacks
  - scripted attacks
  - hardware attacks
  - attacks against Wi Fi
- cyber security risks
- methods of testing systems, networks and applications and confirming incidents
- common procedures in:

  - following organisational cyber security incident response plans
  - responding to cyber security incidents
- legislative requirements applicable to identifying and reporting cyber security incidents
- organisational policies and procedures applicable to cyber security incidents, including:
  - documenting established requirements, incidents and work performed
  - security procedures
  - obtaining and analysing system, network and application information
  - cyber security incident response processes and plans
  - establishing reporting procedures.

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:

- required hardware, software and its components
- system, network and application infrastructure and logs
- the internet
- organisational security procedures including incident response plans.

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