Australian Government

Assessment Requirements for BSBXCS304 Apply cyber hygiene best practices

Release: 1

Assessment Requirements for BSBXCS304 Apply cyber hygiene best practices

Modification History

Release	Comments
Release 1	This version first released with the Business Services Training Package Version 8.0. Newly created unit.

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 use the following cyber hygiene best practices:
  - implement at least three different low impact security measures
  - identify and report at least two phishing emails.

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:

- common cyber hygiene practices surrounding hardware, software, applications, and processes used in own role
- organisational policies and procedures relevant to identifying and using cyber hygiene best practices, including:
  - reporting procedures regarding phishing emails
  - password updates
  - permissions and restricted access to servers
- common indicators of phishing emails, including:
  - grammar and spelling errors
  - inconsistencies in email addresses, links, and domain names
  - suspicious attachments and uniform resource locators (URLs)
  - requests for credentials, payments and personal details
- common cyber hygiene issues, including:
  - loss of data
  - misplaced data
  - security breaches

  - outdated software
  - lack of risk management procedures
- organisational cyber hygiene best practices, including:
  - complex and strong passwords and multifactor authentication
  - updating system software
  - backing up data
  - limiting user permissions and access to applications, systems, and data
  - installation and maintenance of malware detection software and signatures
  - software evaluation and management processes
  - firewalls and demilitarised zone (DMZ) networks
  - vulnerability scans
  - daily full backups
  - weekly incremental backups
- techniques to evaluate and determine cyber hygiene practices.

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 their components
- system, network and application infrastructure
- internet connection that supports the requirements set out in the performance evidence
- organisational security policies and procedures.

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=11ef6853-ceed-4ba7-9d87-4da407e23c10