Australian Government

Assessment Requirements for BSBXCS301 Protect own personal online profile from cyber security threats

Release: 1

Assessment Requirements for BSBXCS301 Protect own personal online profile from cyber security threats

Modification History

Release	Comments
Release 1	This version first released with BSB Business Services Training Package 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:

- conduct one audit of own personal online profile and identify existing and potential cyber security threats
- identify and address three potential cyber security risks to own personal online profile.

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:

- legislative requirements relating to reporting cyber security threats
- organisational policies and procedures relating to online profiles, including escalation routes for cyber security issues
- basic principles of cyber security, including:
  - importance of data confidentiality, integrity and availability
  - common cyber security terms
  - common cyber security threats that individuals might be exposed to online
  - secure internet browsing
- risk factors relating to own personal online profile, including:
  - password management practices:
    - strength of created passwords
    - number of passwords used for multiple accounts
    - frequency of change to passwords
  - own work role within organisation
  - regular tasks in own work that raise personal risk level, including internet browsing
  - potential targets for cyber attack in own direct professional network
  - protocols for handling personally identifiable information

© Commonwealth of Australia, 2024 Future Skills Organisation

    - physical safety of devices
- industry-specific risk factors and their risk to online profiles
- common strategies, tools and techniques for improving security of own personal online profile, including for:
    - password protection
    - secure password management and account replicating and splitting
    - fundamentals of two-factor authentication
    - billing and account privacy settings
    - software patching
    - connecting to public Wi-Fi via virtual private networks (VPNs)
- common methods and practices for:
    - responding to cyber security issues, including reporting protocols
    - secure internet browsing, including banking and email
- common cyber security threats that individuals and data might be exposed to, including:
    - phishing
    - social engineering
    - social media
    - malware
    - physical threats, including data loss due to working insecurely in public spaces.

Assessment Conditions

Skills must be assessed in a workplace or simulated environment where conditions are typical of a work environment requiring cyber secure practices, processes and procedures.

Access is required to:

- information and data sources relating to cyber security
- device with active internet connection
- internet browser
- industry standards and organisational procedures required to demonstrate the performance evidence.

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

© Commonwealth of Australia, 2024 Future Skills Organisation