Assessment Requirements for BSBXCS303 Securely manage personally identifiable information and workplace information

Assessment Requirements for BSBXCS303 Securely manage personally identifiable information and workplace information
document was generated: 21 June 2022

Date this

Assessment Requirements for BSBXCS303 Securely manage personally identifiable information and workplace information

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:

- use data protection techniques to manage workplace information for one work area over the life of a small project or work cycle.

In the course of the above, the candidate must store and share personally identifiable information (PII) in a secure manner.

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 securely managing PII and workplace information, including:
  - data protection
  - implications of Notifiable Data Breach legislation on an organisation and other associated Australian privacy laws
  - established international legislation
- organisational policies and procedures relating to:
  - identifying sensitive data
  - securely storing, sharing and managing customer information
  - encryption, and protocols for its uses
  - data classification
  - media and document labelling
  - monitoring and reporting faults and malfunctions in IT infrastructure
- industry best practice and Australian government sources of information relating to access control, including:

- password protection
- storage locations
- securely sharing
- data deletion
- risks and benefits of cloud storage
- risks of communicating sensitive information via non-secure means e.g. email and SMS
- framework for distributed storage
- technologies, techniques and protocols for storing and retrieving data
- data protection protocols and industry-standard compliance standards relating to:
  - back-up
  - data sharing
  - data storage
  - disposal of sensitive information
  - privacy impact assessments.

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, organisational procedures, and legislative requirements 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