



Australian Government

BSBXCS306 Apply own techniques to prevent cyber security insider threats

Release: 1

BSBXCS306 Apply own techniques to prevent cyber security insider threats

Modification History

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

Application

This unit describes the skills and knowledge required to contribute to business operations through the application of techniques to prevent insider threats in own work. This includes analysing one's own existing strategies to prevent insider threats, and determining and implementing effective insider threat prevention techniques.

The unit applies to individuals in a range of industries and job roles who contribute to the prevention of insider threats as part of broader responsibilities. Individuals will typically work in administrative roles under supervision.

No licensing, legislative or certification requirements apply to this unit at the time of publication.

Unit Sector

Digital Competence - Cyber Security

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
<i>Elements describe the essential outcomes.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element.</i>
1. Prepare to apply techniques to prevent insider threats	1.1 Identify basic insider threat prevention techniques according to organisational security procedures 1.2 Consult with colleagues and stakeholders on insider threats and risks faced by organisation 1.3 Identify frequency, type and impact of insider threats faced in own work area
2. Implement techniques to prevent insider threats	2.1 Consult with colleagues and stakeholders on different prevention

in own work	techniques 2.2 Identify techniques to prevent insider threat according to organisational context 2.3 Administer insider threat prevention techniques to relevant organisational equipment and devices 2.4 Document administered techniques according to organisational policies and procedures 2.5 Provide feedback to required personnel on implemented techniques
3. Review and update insider threat-prevention techniques	3.1 Participate in required organisational learning and development programs regarding insider threat prevention techniques 3.2 Identify insights from training and share benefits to organisation with required personnel 3.3 Update own insider threat prevention techniques where required

Foundation Skills

This section describes those language, literacy, numeracy and employment skills that are essential to performance but not explicit in the performance criteria.

Skill	Description
Reading	Identifies documents and texts of varying complexity to extract and analyse relevant information
Writing	Uses industry-specific and organisational terminology in workplace documents that identify insider threat prevention techniques
Initiative and enterprise	Takes responsibility for identifying effective insider threat prevention techniques in own work context
Technology	Uses technology to access and filter data and then extract, organise, integrate and share information

Unit Mapping Information

No equivalent unit. Newly created unit.

Links

Companion Volume Implementation Guide is found on VETNet - -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=11ef6853-ceed-4ba7-9d87-4da407e23c10>

Assessment Requirements for BSBXCS306 Apply own techniques to prevent cyber security insider threats

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:

- apply techniques to prevent at least two potential cyber security insider threats in own work area, using different techniques with each threat.

In the course of the above, the candidate must:

- adhere to organisational security procedures regarding cyber security insider threat prevention.

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:

- definition of cyber security insider threat
- organisational security procedures for preventing cyber security insider threats
- types of cyber security insider threats and risks, including malicious and accidental actions
- opportunities for insider threats, including:
 - simple passwords
 - orphaned accounts
- human resource policies that support prevention of cyber security insider threats, including:
 - general data protection policies
 - incident response policies
 - third-party access policies
 - account management policies
 - user monitoring policies

- password management policies
- techniques to reduce cyber security insider threats, including:
 - organisation-wide participation in cyber security insider threat awareness programs
 - limiting user permissions and access to applications, systems, and data
 - firewalls and demilitarised zone networks
 - software monitoring
- good practice examples of organisational learning and development programs regarding insider threat prevention.

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 cyber security policies and procedures
- legislative requirements regarding organisational security.

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>