



Australian Government

BSBXCS401 Maintain security of digital devices

Release: 1

BSBXCS401 Maintain security of digital devices

Modification History

Release	Comments
Release 1	This version first released with BSB Business Services Training Package 6.0.

Application

This unit describes the skills and knowledge required ensure the cyber security of digital devices.

It applies to those working in a broad range of industries who as part of their job role ensure the security of digital devices used.

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. Identify appropriate security for digital devices	1.1 Create and maintain register of digital devices on organisation's network 1.2 Confirm what information is held on the registered devices 1.3 Categorise level of risk associated with each device based on sensitivity of information stored 1.4 Select required security protocol to manage level of risk associated with each device
2. Apply protection strategies to digital devices	2.1 Install and run latest anti-malware on each device 2.2 Create strong passwords across personal and work accounts 2.3 Switch on two-factor authentication where available

ELEMENT	PERFORMANCE CRITERIA
	2.4 Encrypt devices according to instructions 2.5 Develop associated physical security plan and communicate this to whole organisation
3. Evaluate effectiveness of applied protection strategies	3.1 Review number of breaches and business impact over review period 3.2 Monitor latest developments in digital security 3.3 Support organisation to select most appropriate security strategies
4. Patch software across multiple devices	4.1 Apply updates to software and applications across own desktop and mobile devices 4.2 Ensure that new devices are updated and configured correctly as part of initial start-up procedure

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
Learning	Modifies behaviour following exposure to new information
Numeracy	- Interprets mathematical data - Completes at times complex calculations and records mathematical data
Reading	Recognises and interprets information from relevant sources to determine organisational expectations relating to cyber security
Technology	Uses appropriate technology platforms to assist with protection strategies relating to cyber security

Unit Mapping Information

No equivalent unit. New unit.

Links

Companion Volume Implementation Guide is found on VETNet: -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>

Assessment Requirements for BSBXCS401 Maintain security of digital devices

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 best practice protection strategies to maintain the security of two different electronic devices over the life of a small project or work cycle
- conduct gap analysis to evaluate effectiveness of all applied best practice strategies.

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:

- external party security risks and methods for mitigating risk
- industry-accepted best practice protection strategies for improving security on digital devices:
 - password management
 - use of anti-virus software
 - virtual private network (VPN) use on public Wi-Fi
 - router settings
 - fundamentals of two-factor authentication
 - encryption
 - patching software applications
- risk management methodologies
- tools and techniques to conduct gap analysis of strategy performance
- data protection requirements for:
 - stored data
 - data in transit
 - data in third party applications
- mobile device security strategies.

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>