



Australian Government

BSBXCS304 Apply cyber hygiene best practices

Release: 1

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.

Application

This unit describes the skills and knowledge required to identify and use organisational cyber hygiene best practices to ensure that users of computers and other devices maintain system health and online security.

The unit applies to individuals working in a broad range of industries and job roles who engage with and use computers and other devices.

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 and prepare to use organisational cyber hygiene best practices	1.1 Identify organisational priorities regarding cyber hygiene 1.2 Identify organisational cyber hygiene best practices to incorporate into own practices 1.3 Prepare appropriate organisational cyber hygiene practices relevant to own role and workplace according to organisational policies and procedures
2. Implement organisational cyber hygiene best practices in own workspace	2.1 Identify and remove obsolete programs and fragmented files from workplace devices according to organisational policies and procedures 2.2 Identify and report phishing emails according to organisational policies and procedures

	2.3 Apply complex passwords and multifactor authentication to devices according to organisational policies and procedures 2.4 Update software if required by organisation
3. Evaluate and update organisational cyber hygiene best practices	3.1 Participate in required learning and development relating to organisational cyber hygiene best practice 3.2 Review application of own organisational cyber hygiene practices 3.3 Update organisational cyber hygiene practices as required own review and by organisation

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 regarding cyber hygiene best practice - Develops basic understanding of trends in cyber security protection
Reading	Identifies and interprets information from relevant sources to determine practices for optimal cyber health
Writing	Uses clear and industry-specific terminology relating to cyber hygiene
Initiative and enterprise	Proactively incorporates cyber hygiene best practice into daily routine
Planning and organising	Manages own cyber hygiene plan that emphasises the importance of carrying out regular, low impact security measures, such as password change or multifactor authentication
Technology	Uses appropriate technology platforms to assist with cyber hygiene best practice

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 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>