



Australian Government

BSBXCS407 Develop cyber hygiene best practice plan

Release: 1

BSBXCS407 Develop cyber hygiene best practice plan

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 develop a plan to incorporate cyber hygiene best practices within an organisation. This includes analysing the existing organisational approach to cyber hygiene and drafting a plan to develop new practices.

The unit applies to individuals in specialist positions who are required to contribute to the development of cyber hygiene best practices as part of broader responsibilities.

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 develop cyber hygiene best practice plan	1.1 Research cyber hygiene best practices 1.2 Identify strengths and weaknesses of cyber hygiene practices in own organisation 1.3 Assess employee awareness surrounding cyber hygiene practices
2. Analyse organisation's past record of cyber hygiene and breaches	2.1 Analyse historical data on organisational cyber breaches 2.2 Analyse historical data on changes in organisational cyber hygiene practices 2.3 Assess regularity of breaches and identify relationships between updates in cyber hygiene and regularity of breaches
3. Develop cyber hygiene	3.1 Use primary and secondary resources to gather a range of

best practice plan for organisation	information on organisational cyber hygiene best practice 3.2 Draft a cyber hygiene best practice organisational plan based on previously identified failures and successes and according to legislative requirements
4. Update and finalise cyber hygiene best practice plan	4.1 Seek feedback on draft cyber hygiene best practice plan from required personnel according to organisational policies and procedures 4.2 Integrate feedback and finalise plan 4.3 Seek plan sign-off according to organisational policies and procedures 4.4 Distribute and store documented plan according to organisational policies and procedures

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	Selects, synthesises, and evaluates evidence from a range of sources
Writing	- Develops written texts using appropriate grammar, spelling and punctuation in relevant organisational formats - Uses clear and industry-specific terminology relating to cyber hygiene
Problem solving	Uses problem-solving skills to identify and analyse issues or barriers, consider options and develop responses and opportunities for improving cyber hygiene
Technology	Uses appropriate technology platforms to assist with developing plan

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 BSBXCS407 Develop cyber hygiene best practice plan

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:

- develop and seek feedback on at least one cyber hygiene best practice plan.

In the course of the above, the candidate must:

- analyse historical organisational cyber security data.

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:

- organisational policies and procedures relating to cyber hygiene practices and plans
- legislative requirements relevant to cyber hygiene practices
- consequences of poor cyber hygiene practices
- historical data relevant to plan development, including relationship between cyber breaches and implementation of best practice methods
- methods to collect information from primary and secondary resources on cyber hygiene best practice
- common cyber hygiene issues, including:
 - loss of data
 - misplaced data
 - security breaches
 - outdated software
 - old security software
 - lack of risk management strategies
- cyber hygiene practices, including:

- complex and strong passwords
- multifactor authentication
- software updates
- backing up data
- limiting user permissions and access to applications, systems, and data
- firewalls
- phishing email alerts
- multifactor and complex passwords
- regular data backups
- antivirus software
- organisational format and features expected of cyber hygiene best practice plans.

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
- 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>