BSBXCS402

Promote workplace cyber security awareness and best practices

Assessment 4 of 6

Project

Assessment Instructions

Task overview

Read the instructions carefully before typing your response in the space provided.

Additional resources and supporting documents

To complete this assessment, you will need:

- Learning Resources
- CBSA Policy and Procedure Template
- CBSA Information Technology Policy and Procedures
- CBSA Style Guide

Assessment Information

Submission

You are entitled to three (3) attempts to complete this assessment satisfactorily. Incomplete assessments will not be marked and will count as one of your three attempts.

All questions must be responded to correctly to be assessed as satisfactory for this assessment.

Answers must be typed into the space provided and submitted electronically via the LMS. Hand-written assessments will not be accepted unless previously arranged with your assessor.

Reasonable adjustment

Students may request a reasonable adjustment for assessment tasks.

Reasonable adjustment usually involves varying:

- the processes for conducting the assessment (e.g. allowing additional time)
- the evidence gathering techniques (e.g. oral rather than written questioning, use of a scribe, modifications to equipment)

However, the evidence collected must allow the student to demonstrate all requirements of the unit.

Refer to the Student Handbook or contact your Trainer for further information.

Please consider the environment before printing this assessment.

Case Study

For the purpose of this assessment, you will play the role of Tan Yamamoto (Software Developer in the IT team at Complete Business Solutions Australia CBSA.

You have been tasked by Con Kafatos, head of IT, to develop a Cybersecurity Awareness Program. Read Con's Email below:

To: Tan Yamamoto (tan.yamamoto@cbsa.com.au)

From: Con Kafatos (con.kafatos@cbsa.com.au)

Date/time: Monday 9:52 a.m.

Subject: Develop a Cybersecurity Awareness Program

Good morning Tan,

A. Thanks for leading the consultation session the other day.

B. I would now like you to develop a Cybersecurity Awareness Program which consists of the following:

- Cybersecurity Awareness Policy and Procedures
- Training for this policy and procedures.

I will be tasking you to deliver this training at a later date.

I also want you to review the existing Information Technology Policy and Procedures as it is related to the cybersecurity awareness program and update this to address any cybersecurity issues.

Please ensure that you use the CBSA Policy and Procedure template when developing the Cybersecurity Awareness Policy and Procedures and that you always comply with CBSA's Style Guide.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

Task 1

A. Using the Policy and Procedure Template, develop a Cybersecurity Awareness Policy and Procedure that:

- specifies an appropriate name for the policy
- specifies a relevant purpose for the policy under the Purpose heading
- specifies relevant information about the policy under the Policy heading
- specifies at least two procedures concerning two different cybersecurity matters
- complies with CBSA's Style Guide.

- submit the document along with the assessment using the following naming convention:

  <StudentNumber>Cybersecurity Awareness Policy and Procedure

B. Create a **Training Session Plan** to organise the delivery of your training in the template provided below. Organise your training to run for approximately 15 - 20 minutes.

C. Update the existing CBSA Information Technology Policy and Procedures to address any cybersecurity issues. You must:

- document at least two updates to improve this policy/procedure, making it clear where these updates have been made (use a different colour font or similar)
- comply with CBSA's Style Guide.
- submit the document along with the assessment using the following naming convention:

  <StudentNumber> CBSA Information Technology Policy and Procedures – UPDATED

Session Overview [Approximate word count: 20 – 30 words]	*The program aims to instil a robust understanding of cybersecurity principles, reinforce the importance of adhering to cybersecurity policies and procedures, and fortify our defences against evolving cyber threats.*		
Session Objectives [Identify one (1) objective]	1. *Familiarise participants with the importance of cybersecurity and its relevance to our organisation.* 2. *Develop a clear understanding of the CBSA Cybersecurity Awareness Policy and Procedures.* 3. *Equip participants with the knowledge and skills to implement and adhere to the Cybersecurity Awareness Policy and Procedures.*		
Topics {Provide at least two (2) topics]	**Breakdown** [Explain what you will cover in each topic in 15 – 20 words]	**Time allocated** [Insert the amount of time you will need to cover each topic]	**Resources required** *(computer/projector, videos, links etc.)*
Introduction to Cybersecurity Awareness	• Welcome and Icebreaker • Overview of the Cybersecurity Threat Landscape • Importance of Cybersecurity in Our Organisation	5 mins	• Computer • Projector • Cybersecurity Awareness Policy and Procedure
Cybersecurity Awareness Policy and Procedures	• Welcome and Icebreaker • Overview of the Cybersecurity Threat Landscape • Importance of Cybersecurity in Our Organisation	5 mins	• Computer • Projector • Cybersecurity Awareness Policy and Procedure

Training on Cybersecurity Policy and Procedures	• Practical Exercises • Role-playing and Simulations • Assessment and Feedback	10 mins	• Computer • Projector • Cybersecurity Awareness Policy and Procedure

Assessor instructions: The purpose of this task is to assess the student's ability to:

- create a cyber security awareness program that reflects organisation-wide best practice
- review cyber security practices according to organisational policies and procedures
- contribute to developing cyber security policies and procedures
- develop one set of policies and procedures for a work area that promotes cyber security awareness and practices.

More specifically, the student:

- Provided a relevant name, purpose, policy and two procedures as per the sample provided.
- Create a training session plan using the template provided.
- Provided at least two updates to the existing Information Technology Policy and Procedures to address cybersecurity matters that are identifiable (different font colour, for example).

An example solution using the CBSA Policy and Procedure Template is provided below;

Cybersecurity Awareness Policy and Procedures

Purpose

This policy is designed to raise the awareness of all employees to cybersecurity threats.

Policy

CBSA's cybersecurity awareness policy outlines the following security measures:

- ensuring policies and procedures are up to date
- email security measures
- keeping data confidential
- incident response
- internet and social media usage standards
- protecting company devices
- recognising the latest cybersecurity threats
- regular backups of organisational data.
- transferring data securely

- using automated anti-malware and network monitoring software
- using strong passwords.

Procedures

The student must list at least two from the examples provided below.

1. Strong password:
   a) User passwords must be at least eight characters long.
   b) Must contain at least one lower case character, one upper case character, and one number.
   c) Must be different from your previous password.
   d) Must not contain any personal information such as your name or date of birth.
2. Spam emails:
   a) Before opening an email ensure that you check who it is from.
   b) If you don't recognise the sender, look for the following suspicious identifiers:
      – Email address is from another country.
      – Email address name doesn't match the email address.
        For example, states it is coming from Microsoft, but the email address is not Microsoft.
      – Subject lines contain strange characters or poor English grammar.
      – If you spot any of these suspicious identifiers, don't open the email and contact IT support as soon as possible.
3. Use of external hard drive/USB:
   a) Before using an external portable hard drive such a USB, get it tested by the IT Team.
   b) Do not use any external device for copying and transferring information between staff.
   c) Any confidential or CBSA document should not be copied on to any external USB or hard drive.

The student should review the CBSA Information Technology policy and procedure and suggest updates as per the procedures included in the cybersecurity awareness policy and procedure.

As per the sample provided for the assessor, the following procedures in the information technology policy and procedure can be updated by the students. Points 1.4 and 2.3 have been added. See below:

1. Accessing the computer system:

1.1. Login instructions.

1.1.1. Each staff member will be provided with a personal login and password for the computer system.

1.2. Keep passwords secure.

1.2.1. Passwords are to be kept secure and private at all times.

1.3. Deactivate passwords at the end of employment.

1.3.1. At the end of employment these passwords will be deactivated.

1.4 Staff need to create a strong password which includes: (added as sample response)

1.4.1. User passwords must be at least eight characters long.

1.4.2. Must contain at least one lower case character, one upper case character, and one number.

1.4.3. Must be different from your previous password.

1.4.4. Must not contain any personal information such as your name or date of birth.

Accessing emails:

2.1. Email address instructions.

2.1.1. All staff will be issued with an email address upon induction.

2.1.2. The email account must be used in strict accordance with the Information Technology Policy.

2.1.3 Any emails should conform to the Email Template requirements.

2.2. Ensure email signature is included in outgoing emails.

2.2.1. All outgoing mail is to include the standard organisational email signature with the relevant details of the staff member included.

2.2.2. The signature will include the standard disclaimer.

2.3. Spam emails (added as sample response).

2.3.1. Before opening an email ensure that you check who it is from.

2.3.2. If you don't recognise the sender, look for the following suspicious identifiers:

Email address is from another country.

Email address name doesn't match the email address. For example, states it is coming from Microsoft, but the email address is not Microsoft.

Subject lines contain strange characters or poor English grammar.

If you spot any of these suspicious identifiers, don't open the email and contact IT support as soon as possible.

Assessment checklist:

Students must have completed all questions within this assessment before submitting. This includes:

1	Task 1 ▪ Cybersecurity Awareness Policy and Procedures ▪ Training Session Plan ▪ Information Technology Policy and Procedures – UPDATED	☐ ☐ ☐

Congratulations you have reached the end of Assessment 4!