|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Student Name |  | Student Number | |  |
| Unit Code/s & Name/s | BSBXCS402 Promote workplace cyber security awareness and best practices | | | |
| Cluster Name  *If applicable* | N/A | | | |
| Assessment Name | Cyber Security Policy | Assessment Task No. | | 2 of 2 |
| Assessment Due Date |  | Date submitted | | / / |
| Assessor Name |  | | | |
| **Student Declaration:** I declare that this assessment is my own work. Any ideas and comments made by other people have been acknowledged as references. I understand that if this statement is found to be false, it will be regarded as misconduct and will be subject to disciplinary action as outlined in the TAFE Queensland Student Rules. I understand that by emailing or submitting this assessment electronically, I agree to this Declaration in lieu of a written signature. | | | | |
| Student Signature |  | | Date | / / |

|  |  |
| --- | --- |
| **Instructions to Student** | **General Instructions:**  This written assessment contains three (3) parts:   1. Part 1 - Develop a policy and procedure document for cyber security 2. Part 2 - Arrange training for awareness in 3. Beware of phishing 4. Implications of Notifiable Data Breach on the organisation 5. Part 3 - Review current cyber-threats   The answers required for these tasks shall be written in plain English, using language that is understandable by a person of a technical level suitable for the case study.  **Materials to be supplied:**  For the student to successfully complete this assessment they will need to acquire:  A computer system installed with a current desktop operating system with appropriate internet browser, and office suite able to save in Microsoft Word .docx format, and current industry standard file formats  Internet access  Uptown IT documentation, located in the course hub in Connect    **Work, Health and Safety:**  TAFE Queensland student rules are designed to ensure that learners are aware of their rights as well as their responsibilities. All learners are encouraged to familiarise themselves with the TAFE Queensland student rules, specifically as they relate to progress of study and assessment guidelines.  Student rules: <http://tafeqld.edu.au/current-students/student-rules/>  **Assessment Criteria:**  To achieve a satisfactory result, your assessor will be looking for your ability to demonstrate the following key skills/tasks/knowledge to an acceptable industry standard:  Knowledge for creating cyber security policy and procedure documentation.  Knowledge and understanding to create a training session.  Understanding the process in identifying current cyber threats.  Ability to identify the types of risks related to the workplace cyber security. |
| **Submission details** (if relevant) | **Due:** Week 16 as per the unit study guide  Insert your details on page 1 and sign the Student Declaration. Include this form with your submission.  Submit the listed files below as per the instructions in the Connect online learning system stated on the Assessment Task 1 page.  You are to submit three (3) files:   1. BSBXCS402\_AT2\_Part1\_yourName.docx 2. BSBXCS402\_AT2\_Part2\_yourName.zip 3. BSBXCS402\_AT2\_Part3\_yourName.docx   TAFE Queensland Learning Management System:  Connect url: <https://connect.tafeqld.edu.au/d2l/login>  Username; 9 digit student number  For Password: Reset password go to: <https://passwordreset.tafeqld.edu.au/default.aspx>> |
| **Instructions to Assessor** | **Student will require:**  Computer applications currently used in industry  Support resources, including online, manuals and training booklets  A computer system with a suitable current OS and access to the internet  **Work, Health and Safety:**  TAFE Queensland student rules are designed to ensure that learners are aware of their rights as well as their responsibilities. All learners are encouraged to familiarise themselves with the TAFE Queensland student rules, specifically as they relate to progress of study and assessment guidelines.  Student rules: <http://tafeqld.edu.au/current-students/student-rules/>  **Level of Assistance:**  Teachers and tutors should be available in class, and accessible by email for students working from home. Staff cannot directly show students answers but guide them to where to go to complete tasks individually. The teacher will make reasonable adjustment for students, as and when appropriate, after consultation with the Disability and Counselling team.  **Assessment Criteria:**  See Marking Criteria on Connect  Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.  Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards. |
| **Note to Student** | An overview of all Assessment Tasks relevant to this unit is located in the Unit Study Guide. |

## Assessment Task 2

This assessment is in three (3) parts:

1. Develop a policy and procedure document for cyber security
2. Arrange training for awareness in:
3. Beware of phishing
4. Implications of Notifiable Data Breach on the organisation
5. Review current cyber-threats.

In this assessment task, the client is the organisation you work for. Although Uptown IT is at the forefront in helping to support clients in all different facets of IT, the organisation itself has been a bit busy taking care of itself.

One of the senior staff members has noticed that the organisation does not have a policy and procedure document for cyber security and thinks it would be a good time now to develop one that will suit ourselves and something we could market to clients.

The current organisations IT infrastructure is as such:

Diagram

Description automatically generated

© TAFE Queensland

**Your Role**

Senior IT Professional

**Your Organisation**

Uptown IT

Unit 3, 13 Upmost Street

Shelley Shores QLD 4651

Phone: 07 4123 8910

Facsimile: 07 4123 6789

Email: support@uptownit.com.au

**PART** 1 - Developing Cyber Security Policy and Procedure document for Uptown IT

After reviewing the current cyber security policy in Assessment Task 1, you now need to apply the information gathered in Assessment 1 and develop a Cyber Security Policy and Procedure document for Uptown IT.

This new Cyber Security Policy and Procedure document will need to cover:

1. Cyber security:
2. What it is - explain what is cyber security and the topics that are included under cyber security.
3. Establish which Australian and international legislation are applicable to the organisation and why
4. Australian government current information on threats
5. The risks on the organisation associated with cyber security.
6. The policies that need to be in place for:
7. For individuals
8. The network
9. The cloud applications.
10. The procedures to enact the policies
11. Implementing, promoting, and maintaining workplace cyber security:
12. Approaches
13. Practices, to include implementation and maintaining cyber security awareness
14. Verify that the approaches and practices are to an industry standard by discussing these with a stakeholder (teacher or supervisor, colleague, or family member) and having them sign in a signature panel in your document. This is required.

Note: Although this new policy and procedure documentation is for Uptown IT, it will also be used in the future as a template for the organisation’s clients. Therefore, the document needs to be written in a language and format that is understood by clients whose IT knowledge is not as advanced as the staff employed at Uptown IT.

All documentation must abide by the Uptown IT Client Documentation Style Guide.

Document to be created using the Uptown IT style guide

**New document needs to have an appropriate cover page with**:

• correct Upton IT logo

• “Cyber Security Policy and Procedure” title

• Version number and date

Save this document as **BSBXCS402\_AT2\_Part1\_yourname.docx**

**PART 2 – Training**

**You can create this training as a PowerPoint presentation, using Adobe Spark or other software programs that you have.** **Your presentation should have between 8 – 10 slides.**

For this part of the assessments, you need to:

* review the current cyber security in the workplace:
* arrange two (2) separate training programs that will cover the following,

1. Beware of phishing, this to include:
2. Training session – time, topics covered, resources needed
3. Training material – handouts, guide - should include screenshots to help with understanding the topic
4. Simulated activity –could include showing an email that is suspect, how to tag the email as SPAM, what to do afterward. **This activity will be a video recording or an audio/voice over your content**
5. Implications of Notifiable Data Breach on the organisation
6. Training session - time, topics covered, resources
7. Training material – guide of do’s and don’ts
8. Simulated activity – show Australian Government - Office of the Australian Information Commissioner - Notifiable data breaches website. **This activity will be a video recording or an audio/voice over your content**

Each training program needs to cover:

* the basics of what each subject is,
* how to make sure procedures are followed,
* how to keep current with cyber security threats

As with the new Cyber Security Policy and Procedure document, these training programs will also be used with clients in the future, so please keep IT jargon to a minimum.

Document to be created using the Uptown IT style guide

New document needs to have an appropriate cover page with:

• correct Upton IT logo

• “Cyber Security Policy and Procedure” title

• Version number and date

**What to upload for Part 2 – Training session. Each training session will consist of:**

* Presentation
* Handout material
* Simulated activity – video or an audio

Save all your documentation in a compressed file called **BSBXCS402\_AT2\_Part2\_yourname.zip**

**PART 3 - Current cyber threats**

For the last part of the assessment, you will need to review the **current cyber threats** reported in the industry and the types of risks related to workplace cyber security.

The document will include:

1. Current threats
2. Identify the current Australian government sources
3. Identify and describe what the current threats are.
4. Identify the associated risks to the current Uptown IT infrastructure regarding the current cyber threats

* State date listed,
* Alert status
* What the alert is about.

1. Document and present suggested improvements to current organisation cyber security awareness to the stakeholder.

Save this document as **BSBXCS402\_AT2\_Part3\_yourname.docx**

**Submission checklist:**

You are to submit the following three (3) files:

1. BSBXCS402\_AT2\_Part1\_yourName.docx
2. BSBXCS402\_AT2\_Part2\_yourName.zip
3. BSBXCS402\_AT2\_Part3\_yourName.docx