|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 Awareness Portfolio | Assessment Task No. | | 2 of 2 |
| Assessment Due Date | Week 8 | 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 | / / |
| **PRIVACY STATEMENT:** TAFE Queensland is collecting your personal information on this form for the purpose of assessment. In accordance with the Information Privacy Act 2009 (Qld), your personal information will only be accessed by staff employed by TAFE Queensland for the purposes of conducting assessment. Your information will not be provided to any other person or agency unless you have provided TAFE Queensland with permission, if authorised under our Privacy Policy (available at <https://tafeqld.edu.au/global/privacy-policy.html>) or disclosure is otherwise permitted or required by law. Your information will be stored securely. If you wish to access or correct any of your information, discuss how it has been managed or have a concern or complaint about the way the information has been collected, used, stored, or disclosed, please contact the TAFE Queensland Privacy Officer at [privacy@tafeqld.edu.au](mailto:privacy@tafeqld.edu.au) | | | | |

|  |  |
| --- | --- |
| Instructions to Student | General Instructions:  You are employed by Uptown IT and your role is to ascertain the current cyber security awareness in the company, and to contribute to the creation and maintenance of training awareness programs, policies and procedures.  Your teacher/assessor will take on the role of the Project Manager assigned to this project by Uptown IT.  Read the project documentation provided and familiarise yourself with the Project Scenario or Case Study before proceeding with portfolio tasks. Confirm anything you are not sure about with your manager (teacher/assessor). It is essential that you have a clear understanding of the scenario and tasks that you need to complete.  This assessment instrument requires the student to complete a project portfolio that is divided into four (4) parts:  **Part 1:** Establish current level of cyber security awareness and required awareness program  **Part 2:** Support cyber security awareness and organise and review  **Part 3:** Review cyber security awareness in the workplace  **Part 4:** Contingency task and cyber security knowledge.  Materials Required:  You are required to provide your own storage device. The recommendation for this qualification is an external SSD drive with at least 500 GB capacity, if you need to store a copy of the Virtual Machine (VM). For assessment files only, a 64 GB thumb drive will be sufficient  Access to PCs and peripherals – these may differ between classrooms  Access to the internet and browsers  Access to Connect (LMS)  Access to word processing software, such as Microsoft Word  Access to special-purpose tools, equipment, and materials to complete the assessment, for example diagramming software.  Online Delivery:  You must supply your own PC or laptop, peripherals and internet access  You should have permissions and be able to install software on your computer  You will require access to Microsoft Office or similar.  Documentation:  Uptown IT Scenario or Case Study  Uptown IT Cyber Security Audit Report Summary  Uptown IT Cyber Security Solution Template. |

|  |  |
| --- | --- |
|  | 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. Demonstrated ability to:  Establish current level of cyber security awareness in the workplace  Create and maintain appropriate cyber security awareness program in accordance with organisation best practices  Contribute to the creation of cyber security policies and procedures  Liaise with relevant personnel regarding cyber security policies and procedures  Develop, review and maintain cyber security training  Review cyber security practices and assess impact  Review latest cyber security threats and trends  Review current practices and document outcomes  Identify cyber security improvements and communicate them to relevant personnel.  Refer to the marking criteria for specific details:  **BSBXCS402\_AT2\_MC\_TQM\_v2**  Details of location:  TAFE will provide a simulated work environment in the classroom. Research activities may be conducted in the classroom or at home.  If you are unable to attend a scheduled assessment activity, you must notify your teacher before the assessment is due and supply a doctor's certificate and approval from the team manager for an extension.  Time restrictions:  This assignment is designed to take place over 8 weeks or approximately 32 hours. The student is expected to attend classes as per timetable details and should be able to commit up to 3 hours per week of their own time to study or study related activities.  Interactions:  Teamwork skills are essential in the IT industry, therefore you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment tasks individually (unless indicated).  Level of assistance permitted:  Staff cannot directly show students answers or solutions but support and guide them to complete tasks individually. Teachers and tutors should be available in class, and accessible by email for students working from home.  Reasonable Adjustments:  Reasonable adjustments are available to students for a variety of reasons, including: disability, language, literacy and numeracy (LLN) problems or extenuating circumstances. Talk to your teacher, counsellor or disability officer if you require extra support or an extension based on the conditions identified.  Number of Attempts:  You will receive up to two (2) attempts at this assessment task. Should your 1st attempt be unsatisfactory (U), your teacher will provide feedback and discuss the relevant sections / questions with you and will arrange a due date for the submission of your 2nd attempt. If your 2nd submission is unsatisfactory (U), or you fail to submit a 2nd attempt, you will receive an overall unsatisfactory result for this assessment task. Only one re-assessment attempt may be granted for each assessment task.  ***For more information, refer to the Student Rules.***  Work, Health and Safety:  The work environment should be assessed for safety prior to class. Special consideration should be taken regarding potential ICT related hazards such as tripping hazards, electromagnetic radiation, ergonomics and posture. TAFE Queensland health and safety policies and procedures should be followed at all times. |
| **Submission details** (if relevant) | Evidence Required to be Submitted:  Insert your details on the cover page and sign the Student Declaration. Include this template with your submission.  Submission via Connect:  Upload a single file into Assessment 2 (AT2) Assignment Folder in Connect.  Multiple files can be compressed into a single file.  Name the file for Attempt 1 submissions:  BSBXCS402\_AT2\_Surname\_Student Number  Name the file for Attempt 2 submissions:  BSBXCS402\_AT2\_Surname\_Student Number\_R  Assessment to be submitted via:   * TAFE Queensland Learning Management System (Connect): [*https://connect.tafeqld.edu.au/d2l/login*](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*](https://passwordreset.tafeqld.edu.au/default.aspx) |
| Instructions to Assessor | Online Delivery:  Please revise and modify the Instructions to Student section if you are delivering online.  Specifications of assessment:  To be judged competent in this assessment item, the student is required to demonstrate competence in all indicators shown in the marking guide.  Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the web development field of work.  Ensure that students read and familiarise themselves with the Project Scenario and the Client provided relevant files and/or resources before attempting the assessment.  Storage Devices:  Students are required to provide their own storage device. The recommendation for this qualification is an external SSD drive with at least 500 GB capacity, if you need to store a copy of the Virtual Machine (VM). For assessment files only, a 64 GB thumb drive will be sufficient.  Assessor to Provide:  Access to PCs and peripherals – these may differ between classrooms  Access to the internet  Access to Connect (LMS)  Access to word processing software, such as Microsoft Word  Access to special-purpose tools, equipment, and materials to complete the assessment, for example diagramming software.  Online Delivery:  Students to supply their own PC or laptop, peripherals and internet access  Students should have permission and be able to install software on their computer  Students will require access to Microsoft Office or similar  Students will require access to a web server or the ability to install a local web server on their computer (instructions for this will be provided).  Documentation:  Uptown IT Scenario or Case Study  Uptown IT Cyber Security Audit Report Summary  Uptown IT Cyber Security Solution Template.  Level of Assistance Permitted:  Teachers and tutors should be available in class, and accessible by email for students working from home. Staff cannot directly show students answers but support and guide them to complete tasks individually. Students with disability will receive reasonable adjustments.  Interactions:  Teamwork skills are essential in the IT industry, therefore you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment tasks individually (unless indicated).  Contingencies:  Reasonable adjustment is available to students for a variety of reasons, including: disability, language, literacy and numeracy (LLN) problems or extenuating circumstances.  Work, Health and Safety:  The work environment should be assessed for safety prior to class. Special consideration should be taken regarding potential ICT related hazards such as tripping hazards, electromagnetic radiation, ergonomics and posture. TAFE Queensland health and safety policies and procedures should be followed at all times. |
| Note to Student | *An overview of all Assessment Tasks relevant to this unit is located in the Unit Study Guide.* |

|  |  |
| --- | --- |
| Scenario-01 | Scenario |
| **ROLE:** You are employed by Uptown IT and your role is to ascertain the current cyber security awareness in the company, and to contribute to the creation and maintenance of training awareness programs, policies and procedures. Your teacher/assessor will act as your supervising manager.  **UPTOWN IT:**  Uptown IT is a one-stop IT solution provider that includes the following departments:  Management Group  Finance Group  Administration Group  IT Support Group  Web Design Group  Software Development Group.  **THE TASK:**  Management has identified the urgent need to set in place a cyber security awareness program in the company. The decision was made after the results of a recent audit on cyber security awareness exposed a very poor cyber security culture amongst staff members. A summary of the Audit results is presented below.  **CYBER SECURITY AUDIT REPORT SUMMARY:**  Report findings:  1. Some staff members have communicated that they open all emails, including those not originating in the company or from a regular client/partner base  2. Some staff members use their own pen drives and external hard drives to transfer data between work and home – a combination of in-house and remote work modes is currently in place  3. While working remotely, most employees prefer to use their own PC and laptop on their home network instead of company-issued equipment  4. It was observed that at lunchtime, a few people do not lock their workstation screens  5. On a few occasions, staff members communicated that they use their mobile phone data for work-related tasks as they say their internet is faster  6. In two instances, access passwords were displayed on sticky notes placed near the workstations  7. The number of calls for forgotten passwords has increased since introducing the new stricter passwords policy.  A diagram of the company network infrastructure is presented below.    © TAFE Queensland | |

Please use the template provided to complete and submit PARTS 1 to 4.

**BSBXCS402\_UptownIT Cyber Security Solution Template\_SH\_TQM\_v2**

## PART 1 Establish the current level of cyber security awareness and required awareness program

Management has identified the urgent need to set in place a cyber security awareness program in the company. The decision was made after the results of a recent audit on cyber security awareness exposed a very poor cyber security culture amongst staff members.

1. To establish the current level of cyber security awareness in the company, review the audit results presented and identify the areas of cyber security identified by the problems reported, the impact on the workplace, the risk level, and an appropriate training priority.

Each problem reported must be included in the table below.

Areas can include but are not restricted to:

* Phishing attacks
* Removable media
* Passwords and authentication
* Physical security
* Working remotely
* Public Wi-Fi
* Social media use
* Internet and email use
* Social engineering
* Security at home.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Cyber Security Problem | Cyber Security Area | Workplace Impact | Risk Level  (High, Moderate, Low) | Awareness Training Priority (1 Highest – 10 Lowest) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| *Add rows as needed* |  |  |  |  |

1. Communicate with a team member and seek feedback regarding your review and assessment of the audit report and the workplace impact. Document the communication and feedback received and submit it as evidence.
2. Propose a set of cyber security procedures to be included in a company-wide Cyber Security Awareness Policy. Ensure that the procedures proposed cover, as a minimum, all the problems identified in the audit report.
3. For each procedure proposed in 1.3, provide a description of the purpose and content.

|  |  |  |
| --- | --- | --- |
| Proposed Procedure | Purpose | Content Description |
|  |  |  |
|  |  |  |
|  |  |  |
| *Add rows as needed* |  |  |

Your contribution to cyber security policies and procedures consists of selecting one of the procedures proposed in 1.3 and creating the procedure. Use the template provided to write the procedure to ensure compliance with organisational documentation procedures and guidelines. The template is included in the **BSBXCS402\_UptownIT Cyber Security Solution Template\_SH\_TQM\_v2.docx** document.

1. Propose a cyber-security procedures maintenance schedule to review procedures on a regular basis. In the proposal, identify the exceptional circumstances that may trigger an out-of-schedule procedure review.
2. Suggest three (3) strategies for promoting cyber security awareness in the workplace. The strategies proposed must be following organisational policies and procedures.
3. **Conversation with manager**

Arrange a conversation with your manager and seek feedback regarding the following points:

a) The suitability of the procedure that you have written. Modify procedure if required.

b) The proposed maintenance schedule to review cyber security awareness procedures.

c) Discuss and confirm proposed strategies to promote cyber security awareness amongst employees.

Document discussion and confirmed strategies in the Conversation Log.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Conversation Log | | | | |
| Date | Topic | Discussion | Stakeholder | Medium Any oral form of communication, e.g., F2F, Zoom and phone call |
|  |  |  |  |  |
|  |  |  |  |  |
| *Add rows as needed* |  |  |  |  |

## PART 2 Support cyber security awareness and organise and review training

2.1 After reviewing the Cyber Security Audit Report provided in 1.1, you have formed an opinion on the current staff awareness regarding cyber security. You need to arrange two (2) training programs for this task. Select the two areas identified in 1.1 as having the highest priority.

Use the Training Program template provided to ensure compliance with organisational documentation procedures and guidelines. The template is included in the **BSBXCS402\_UptownIT Cyber Security Solution Template\_SH\_TQM\_v2.docx** document.

Each Awareness Training Program must include:

a) Learning objectives

b) Recommended frequency of training

c) Responsibilities

d) Training topic overview

e) Training material

f) Activities

g) Evaluation.

## PART 3 Review cyber security awareness in the workplace

3.1 Use reliable and up-to-date sources to research and review the latest cyber security threats and industry trends. In light of the review, propose at least three (3) improvements that would benefit our company. Identify which procedure(s) must be updated to incorporate the new information. Refer to the procedures proposed in 1.3.

Document the review outcomes in the following table:

|  |  |  |  |
| --- | --- | --- | --- |
| Cyber Security Threat | Trend | Source(s) | Proposed Improvement & Procedure to Update |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

3.2 Communicate with a team member and seek feedback regarding your review and assessment of the latest cyber security threats and trends and your proposed improvements as presented in 3.1.

Document the communication and feedback received and submit it as evidence.

## PART 4 Contingency task and cyber security knowledge

Part 4 requires you to carry out research and provide answers to a number of questions. Provide the answers in your own words. Plagiarism is a form of academic misconduct and will not be tolerated. Include references for all your sources using a formal referencing style such as APA or Harvard.

4.1 **Contingency task** – Outline the processes you would follow if a cyber security issue arises and the company policies do not cover it.

4.2 For each item below, identify what would be the cyber security **legislative requirements** and **implications** in the industry. Provide examples to illustrate your answers.

a) **Data protection** in Australia

b) **Notifiable Data Breach** in Australia

c) **Cyber security** in international legislation affecting Australia

4.3 For each listed policy/procedure, provide the scope of the procedure and three (3) rules or guidelines that should be included to protect the company against cyber security threats.

Provide the answers within the context of the company provided in the scenario.

|  |  |  |
| --- | --- | --- |
| Policy/Procedure For | Scope | Rules/Guidelines  Three (3) for each |
| 1. Securely storing, sharing and managing information |  |  |
| 1. Encryption, and protocols for its uses |  |  |
| 1. Data classification and management |  |  |
| 1. Media/document labelling |  |  |
| 1. Data governance |  |  |
| 1. Acceptable use |  |  |
| 1. Bring your own device |  |  |

**End of Assessment**