|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Student Name | James Eastman | | Student Number | | 467513560 |
| Unit Code/s & Name/s | BSBXCS402 Promote workplace cyber security awareness and best practices | | | | |
| Cluster Name  *If applicable* | N/A | | | | |
| Assessment Type | Assignment  Project  Case Study  Portfolio  Third Party Report (Workplace)  Third Party Report (Peer)  Other | | | | |
| Assessment Name | Cyber security Awareness Portfolio | | Assessment Task No. | | 2 of 2 |
| Assessment Due Date | Week 8 | | Date Submitted | | / / |
| **Assessor Feedback:** | | | | | |
| **Attempt 1** | Satisfactory | Unsatisfactory | | Date | / / |
| Assessor Name |  | | Assessor Signature | |  |
| **Student provided with feedback and reassessment arrangements**  *(check box when completed)* | | | Date scheduled for reassessment | | / / |
| **Attempt 2** | Satisfactory | Unsatisfactory | | Date | / / |
| Assessor Name |  | | Assessor Signature | |  |
| Note to Assessor: Please record below any reasonable adjustment that has occurred during this assessment e.g. written assessment given orally. | | | | | |
|  | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Assessment Criteria / Benchmarks  ***The evidence submitted demonstrates that the student has satisfactorily:*** | Attempt 1 | | Attempt 2 | |
| **Date**  \_\_/\_\_/\_\_ | | **Date**  \_\_/\_\_/\_\_ | |
| Y | N | Y | N |
| PART 1 Establish the current level of cyber security awareness and required awareness program |  |  |  |  |
| 1.1 There is evidence that the review audit summary has been read in light of the answers provided. Cyber security areas affected by the problems described have been identified. For each problem presented:  a) Cyber security area identified |  |  |  |  |
| b) Workplace impact defined |  |  |  |  |
| c) Risk level identified |  |  |  |  |
| d) Required cyber security awareness training identified |  |  |  |  |
| 1.2 Communication with team member seeking feedback regarding review and assessment of the audit report and the workplace impact documented and presented as evidence of communication. |  |  |  |  |
| 1.3 Appropriate security procedures to be included in a company-wide Cyber Security Awareness Policy have been presented. |  |  |  |  |
| 1.4 Each procedure identified in 1.3 includes:  a) Procedure purpose |  |  |  |  |
| b) Procedure content description |  |  |  |  |
| c) One procedure has been selected and created (written) as per template provided. |  |  |  |  |
| 1.5 Proposed cyber-security maintenance schedule to review procedures on a regular basis includes exceptional circumstances that may trigger and out-of-schedule review. |  |  |  |  |
| 1.6 Suggested three (3) strategies to promote cyber security awareness. |  |  |  |  |
| 1.7 Conversation with manager recorded and presented in the Conversation Log for the following topics:  a) Seek feedback regarding the suitability of the procedure written in 1.4 c. Modify procedure if required |  |  |  |  |
| b) Proposed maintenance schedule to review cyber security awareness procedures |  |  |  |  |
| c) Discuss and confirm strategies to promote cyber security awareness amongst employees. |  |  |  |  |
| PART 2 Support cyber security awareness and organise and review training |  |  |  |  |
| 2.1 Two cyber security awareness programs have been created and submitted; each training program includes:  Learning objectives  Recommended frequency of training  Responsibilities  Training topic overview  Training material  Activities  Evaluation.  a) Training program 1 completed |  |  |  |  |
| b) Training program 2 completed |  |  |  |  |
| 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 trends affecting the industry. For each threat identified, provide:  a) Trend |  |  |  |  |
| b) Sources |  |  |  |  |
| c) Proposed improvement |  |  |  |  |
| d) Procedure that needs to be updated |  |  |  |  |
| 3.2 Communication with team member seeking feedback regarding your review and assessment of the latest cyber security threats and trends and your proposed improvements as presented in 3.1 has been documented and presented as evidence of communication. |  |  |  |  |
| PART 4 Contingency task and cyber security knowledge |  |  |  |  |
| 4.1 **Contingency task** – Outline the processes that you would follow if a cyber security issue arises, that is not covered. Appropriate solution presented. |  |  |  |  |
| 4.2 For each item below, the cyber security legislative requirements and implications in the industry have been identified, and examples provided:  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, the scope of the procedure and three (3) rules or guidelines that should be included to protect the company against cyber security threats have been provided.  a) Securely storing, sharing and managing information |  |  |  |  |
| b) Encryption and protocols for its uses |  |  |  |  |
| c) Data classification and management |  |  |  |  |
| d) Media/document labelling |  |  |  |  |
| e) Data governance |  |  |  |  |
| f) Acceptable use |  |  |  |  |
| g) Bring your own device |  |  |  |  |