|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 Type | Assignment  Project  Case Study  Portfolio  Third Party Report (Workplace)  Third Party Report (Peer)  Other | | | | |
| Assessment Name | Cyber Security Policy | | Assessment Task No. | | 2 of 2 |
| Assessment Due Date |  | | 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 | | | | |
| 1. Cyber security |  |  |  |  |
| 1. Identified and explained what cyber security is |  |  |  |  |
| 1. Established the current legislation for cyber security and related Australia and international legislations and provided a reason why each occurs |  |  |  |  |
| 1. Explained the risks associated with cyber security and the organisation |  |  |  |  |
| 1. Identified the policies that need to be in plave for: |  |  |  |  |
| 1. Individuals |  |  |  |  |
| 1. The organisation’s network infrastructure |  |  |  |  |
| 1. Cloud applications |  |  |  |  |
| 1. The procedures to enact the policies identified in 1.2a, 1.2b, 1.2c |  |  |  |  |
| 1. Documented how to implement, promote, and maintaining workplace cyber security by identifying: | | | | |
| 1. Approaches |  |  |  |  |
| 1. And practices, including implementation and maintaining cyber security awareness |  |  |  |  |
| 1. Verified the approaches and practices by discussing these with a stakeholder (teacher or supervisor) and obtaining a verification signature |  |  |  |  |
| PART 2 | | | | |
| 1. Arrange training program for “Beware of phishing”, by producing: | | | | |
| 1. Correctly presented training session |  |  |  |  |
| 1. Relevant training material |  |  |  |  |
| 1. Simulated activity |  |  |  |  |
| 1. Arrange training program for implentations of “Notifiable Data Breach on the organisation”, by producing: | | | | |
| 1. Correctly presented training session |  |  |  |  |
| 1. Relevant training material |  |  |  |  |
| 1. Simulated activity |  |  |  |  |
| PART 3 | | | | |
| 1. Documented the current cyber threats: | | | | |
| 1. Identified the correct current Australian Government source |  |  |  |  |
| 1. Identified and described the current threats |  |  |  |  |
| 1. Identified associated risks to the current Uptown IT infrastructure in regard to the current cyber threats |  |  |  |  |
| 1. Document and present suggested improvements to current organisation cyber security awareness to the stakeholder |  |  |  |  |