Assessment Marking Criteria

BSBXCS402_AT2_MC_TQM_v1

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** **Date** __/__/__		**Attempt 2** **Date** __/__/__	
	Y	**N**	**Y**	**N**
PART 1				
1. Cyber security	☐	☐	☐	☐
a) Identified and explained what cyber security is	☐	☐	☐	☐
b) Established the current legislation for cyber security and related Australia and international legislations and provided a reason why each occurs	☐	☐	☐	☐
c) Explained the risks associated with cyber security and the organisation	☐	☐	☐	☐
2. Identified the policies that need to be in plave for:	☐	☐	☐	☐
a) Individuals	☐	☐	☐	☐
b) The organisation's network infrastructure	☐	☐	☐	☐
c) Cloud applications	☐	☐	☐	☐
3. The procedures to enact the policies identified in 1.2a, 1.2b, 1.2c	☐	☐	☐	☐
4. Documented how to implement, promote, and maintaining workplace cyber security by identifying:				
a) Approaches	☐	☐	☐	☐
b) And practices, including implementation and maintaining cyber security awareness	☐	☐	☐	☐
c) 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:				
a) Correctly presented training session	☐	☐	☐	☐
b) Relevant training material	☐	☐	☐	☐
c) Simulated activity	☐	☐	☐	☐
2. Arrange training program for implentations of "Notifiable Data Breach on the organisation", by producing:				

a)	Correctly presented training session	☐	☐	☐	☐
b)	Relevant training material	☐	☐	☐	☐
c)	Simulated activity	☐	☐	☐	☐
PART 3					
1.	Documented the current cyber threats:				
a)	Identified the correct current Australian Government source	☐	☐	☐	☐
b)	Identified and described the current threats	☐	☐	☐	☐
2.	Identified associated risks to the current Uptown IT infrastructure in regard to the current cyber threats	☐	☐	☐	☐
3.	Document and present suggested improvements to current organisation cyber security awareness to the stakeholder	☐	☐	☐	☐